executive report

ferf
financial executives
research foundation

sponsored by
RR DONNELLEY

INSIGHT ON OUTSOURCED SERVICE PROVIDERS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The very name "internal control" poses a problem for companies when they deal with outsourced providers.[1]

Risk assessment cuts across the entire senior team of an organization, ranging from the board of directors to the C-Suite, and to HR, IT and Finance. Organizations have to account for their various exposures and design programs to mitigate their risks. This is even more pertinent for organizations that choose to outsource certain functions or processes. In particular, utilizing cloud-based service providers and infrastructure to streamline regulatory requirements may expose an organization to unexpected risk.

While enhancing the fundamentals of internal controls over financial reporting (ICFR), the *2013 COSO Framework* casts a wider net to embrace the evolution of cloud-based technology and outsourced infrastructure to streamline and create efficiency in managing the organization's business. The framework includes explicit content in 12 of the 17 principles relating to outsourced service providers (OSPs), outlining where a company should go beyond monitoring the controls to researching its risk tolerance, and assessing the controls of the OSP as they relate specifically to the company's activities.

This Financial Executives Research Foundation (FERF) report, sponsored by RR Donnelley, provides insight into how companies establish internal controls relating to financial reporting and operations over outsourced functions. The FERF staff interviewed preparers, auditors and consultants to help reach its findings.

[1] COSO: Internal control a challenge with outsourced providers, Tysiac, Ken, February 6, 2015 http://journalofaccountancy.com/news/2015/feb/how-to-apply-COSO-to-outsourced-providers-201511682.html

Key findings include:

- There should be "pre-qualifying" work performed to select an OSP that involves consideration of the control environment objectives of the user company. This includes, but is not limited to, research of the OSP, reviewing the ethics code of the OSP, interviewing members of OSP management and assessing whether the corporate culture is in line with the user organization's culture.
- Contracts should be written with specific language that allows the client to invoke a right to audit – using internal auditors or others.
- Many different suggestions in assessing risk were provided. However, the overarching theme is that a risk assessment related to an OSP must be performed by the user organization itself.
- Some suggest starting at the financial statement level (assessing major classes of transactions, assertions and related internal controls) to categorize related OSPs and risk; while another suggests placing OSPs into risk categories or tiers -- where each category will signify work that should be done to mitigate risk associated with the OSP.
- Since OSPs differ, the user organization should not use a *cookie cutter* approach to assess risks.
- Service Organization Controls (SOC)[2] reports are a good *starting point* for assessing the internal controls of the OSPs.
- The user organization should design and implement controls to ensure the information provided to and received from the OSP is accurate.
- If the OSP does not provide a SOC report, the user organization should perform tests of the organization's controls over the OSP activities or perform tests of the OSP's controls.
- User organizations should test the controls they have in place regardless of whether a SOC is provided.
- Communication channels need to be predefined and used regularly. After the prequalifying stage and hiring of an OSP, the OSP may experience an organizational change. Therefore, it is critical to communicate regularly in order to learn about these changes before the next SOC report is received.
- It is important to read and understand the SOC report to ensure that there are no deficiencies or exceptions noted. Should there be any, find out how these have been addressed; if they haven't been addressed, learn how they can be addressed in the future.
- It is critical to be aware of any internal control deficiencies at the OSP and assess whether remediation efforts are in place at the OSP, what controls are in place within the user organization that may address the issues, and whether the OSP deficiencies translate into internal control issues for the user organization.
- User organizations should extend their whistleblower hotline to OSPs.
- A SOC report should not only be reviewed, but the user organization must ensure that any additional information is received (i.e., payroll data). Such additional information should be reconciled to ensure its accuracy and completeness.
- Lines of communication should be kept open. The OSP should notify the user of any organizational changes that may affect the user organization.

[2] For clarification purposes, SOC 1 reports focus on financial reporting risk and controls specified by the service provider and are most applicable when the service provider performs financial transaction processing or supports transaction processing systems. A SOC 2 or 3 report focuses on security, availability, confidentiality, processing integrity, and privacy. Effectively using SOC 1, SOC 2 and SOC 3 reports can increase assurance over outsourced operations, KPMG, 2012.- https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/SOCWhitepaper.pdf

DO YOU CURRENTLY USE AN OSP? IF YES, FOR WHAT AREAS OF FINANCE OR OPERATIONS?

Overall, the use of OSPs is seen as a cost-efficiency strategy, and therefore has been increasing steadily over the past decade. Based on interviews, OSP usage ranges from financial reporting information — such as investments, pensions, tax and payroll — to non-financial information, including logistics, janitorial and even contract labor. A Deloitte survey reveals that technology seems to be the most utilized outsourced service because of widespread technological advancements, such as cloud computing, big data, and mobility process improvements, to name a few[3].

ARE THERE INTERNAL CONTROLS AROUND SELECTING AN OSP? IS THE ETHICAL POSTURE AND CORPORATE CULTURE OF THE OSP CONSIDERED DURING THE SELECTION?

Organizations are performing "pre-qualifying work" to determine whether an OSP is competent and holds the same integrity and ethical values as the user organization. This supports principles 1, 4, and 5 of the *2013 COSO Framework*. Some practices that arose from the interviews included:

- Conducting internet searches of an OSP;
- Reviewing the OSP's code of conduct and policies regarding actions taken when it is not followed, to assess the OSP's tone at the top and whether employees are being held accountable;
- Researching officers and directors at the OSP;
- Interviewing members of OSP's management.
- Involving the company's procurement department; and
- Reviewing cybersecurity policies.

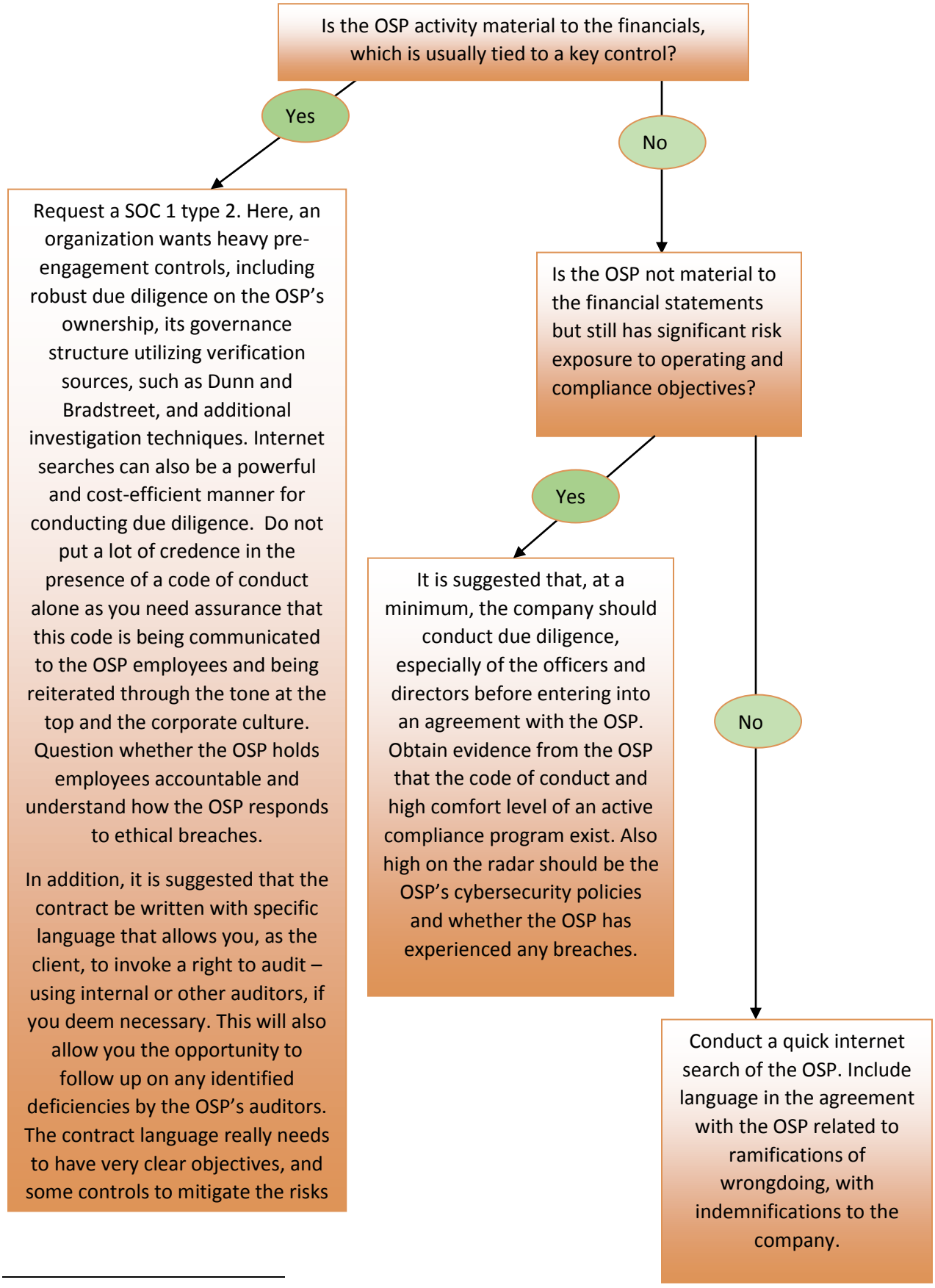
Usage of questionnaires by the user company and an understanding of the OSP's Service Organization Controls (SOC) reports (either 1 or 2) can also help during the selection process.

Our interviewees also emphasized that pre-qualifying work should vary based on the **significance of the risk** of that particular OSP.

For example, if the OSP is material to financial performance, and is tied to key controls, SOC 1 type 2 controls should be requested by the OSP in addition to internal controls. Below is a suggested decision tree to determine the appropriate level of pre-work.

[3] Deloitte's 2014 global outsourcing and insourcing survey, Mancher Marc, 2014
http://www2.deloitte.com/us/en/pages/strategy/articles/2014-global-outsourcing-and-insourcing-survey.html

DECISION TREE: CONSIDERING RISK TO DETERMINE LEVEL OF PREQUALIFYING WORK[4]



[4] Kral, Ron (2015, May 1). Telephone interview.

After the prequalification phase, it is recommended that regular communication channels need to be predefined and set. Oftentimes, after the company's vendor prequalification process, changes may occur. For this reason, companies are advised to periodically revisit the situation and have an open line of communication with the vendor liaison or someone who will hold the OSP accountable for changes to its governance structure and controls. Also, it is critical for OSPs to communicate sooner rather than later if they become aware of a material error or fraud that impacts the service they are providing; they should not wait to communicate until their SOC 1 report is finalized. As Kral says: "You need to set the expectation that your OSP needs to contact you immediately."

Extending the company's whistleblower hotline to the OSPs is critical.[5] "The Association of Certified Fraud Examiners reveals, through periodic surveys, that fraud is detected not just from employee tips, but through vendors, customers and other sources. It is a low cost, easy thing to do to extend your hotline to these other stakeholder groups."

Ron Kral, managing partner at Candela Solutions LLC

There are internal controls around selecting OSPs as well as ethical considerations of the OSPs. "This is handled through a procurement work process in both RFP requirements and contract language, in addition to the affected function assessment. In cases where there is an IT component, the IT work process performs a separate IT security analysis after a provider has been selected."

Member of the Internal Control Compliance team at a chemical company

---

As to the internal controls employed around selecting an OSP, "Whenever we engage a new service provider, our procurement department goes through a fairly robust due diligence process to review OSPs. This diligence process identifies criminal activity, complaints, etc., and also includes analyzing the tone at the top and corporate culture of the OSP."

Senior director of corporate accounting at an electronics manufacturer

---

As part of a standard evaluation process, this chemical manufacturer reviews the OSP's information before engaging the organization. "We have procurement policies that require, among other things, a background check about the provider, industry references, and perhaps an onsite visit. This information is included in a business case that senior management gets heavily involved in. After we have contracted with the OSP, we provide them with access to our internal whistleblower hotline as well, if they have employees working at our sites."

Director of Internal Audit at a chemical manufacturer

[5] For further information, please refer to FERF report - *Breaking the Cycle of Fraud* 2015. www.ferf.org/reports

Speaking from more of an information security perspective and addressing implications on the OSP, one vice president said: “My organization has developed a ‘cloud service policy and standard,‘ formally known as Application Service Provider pre-cloud technology. These policies define how we engage with service providers, which fall within a few options. The first option is that the OSP can choose to adhere to our security standards, which include a set of standards that govern IT and separation of duties (SOD), all the different physical and IT controls, data controls, and protection. The second option is the SOC approach, where they attest to their degree of controls from an industry standard perspective. And the final option is a hybrid between these two. They would need to demonstrate that their security standard is adequate. We would, absolutely, audit this type and if we agree that it is adequate, the OSP would commit to maintaining that level of control and compliance, without deviating and alerting us that they are changing their security standard. Subsequently, this security standard requires, at a minimum, an annual review of the OSP. We have a validation phase that would require the company to go back and periodically review compliance and controls. We have also included in our contracts with the OSP that we have a right to audit them at almost any time.”

VP of finance and IT transformation for a technology company

Providing thought leadership from an information security perspective is recommended. It is suggested that, in addition to getting the data back from the OSs, it is equally important to audit and review information security at the OSP to ensure the information that the company is sending is secure. “We assess risk that any OSP that we may send data to and how they may present risks to the company,” says one analyst. “For example, most of the data our company sends is pre-release financial data so we are ultimately concerned with how the OSP handles and secures this data. We conduct our risk assessment process that all OSPs go through. This risk assessment begins with a questionnaire created based on general experience in the business, familiarity with our product and how our data is being used by our vendors. We look for vendors to answer the questions for us to get comfort. Vendors normally answer these questions with a SOC report. Even though it is a good place to start, the SOC report does not provide enough insight for us to assess risk that may be presented to the company.”

Network security analyst at a restaurant chain

HOW DOES YOUR ORGANIZATION ASSESS RISK OF INFORMATION PROVIDED BY OSPS?

Risk assessment has been the highlight of the *2013 COSO Framework* with the explicit expansion of risk assessment to include consideration of a company's OSP - Principles 6, 7, 8 and 9.

As many have said, "You can't outsource risk to your OSP. Management must consider specific risks that are inherent with choosing and maintaining a relationship with an OSP."

Some key areas of risk range from financial reporting and operational issues, such as application (cybersecurity) and physical security, to business continuity and, in some cases, the financial viability of the OSP. More importantly, it is suggested that assessing risk on a sliding scale rather than as a *cookie cutter* approach is key because the risk profile varies for each OSP.

> "Organizations that have implemented the *2013 COSO Framework* are considering OSPs in their ICFR risk assessment now. Risk assessment starts with the financial statements and drives down into the major classes of transactions, assertions and related internal controls, including those transactions and controls operated by OSPs. Companies can outsource the transactions and controls, but they retain ICFR accountability for them, as such, the same risk assessment process is applied to all relevant transactions and controls – whether insourced or outsourced."
>
> Forewarning of the risk of change, she adds, "Any time you are introducing change, you are introducing an element of risk that needs to be managed."
>
> ***Sandra Herrygers, Deloitte Advisory partner at Deloitte & Touche LLP***

> "We start at the financial statement level and, certainly, payroll expense is a material item to us. The next stage would be to go through and identify the key controls that we are relying upon for that third party, as our key controls extend to our service provider."
>
> ***Senior director of corporate accounting at an electronics manufacturer***

> "Evaluation of OSPs should start with the three broad objectives of the *2013 COSO Framework* and move into a risk assessment looking at the magnitude and the potential errors and fraud, on behalf of the OSP."
>
> Kral's approach is to have his clients divide the OSPs into three categories:
>
> - **Tier 1**: If the OSP is material to the financials, which is usually tied to a key control, then a SOC 1 type 2 is requested.
>
> - **Tier 2**: If the OSP is not material to the financial statements but still has significant risk exposure to operating and compliance objectives, SOC reports are usually note requested. These OSPs would typically be law firms, advisors, consultants, agents, and even sometimes

janitorial services, since they have access to sensitive documents. However, some relatively strong controls are still recommended for this group.

- **Tier 3:** This includes all other service providers that are routine and not material. There are some basic controls and procedures that will apply to them, but they are much more limited than for a Tier 1 or Tier 2 OSP. This group may include delivery service providers, cafeteria services, and others - all with low risk exposures.

A deep dive into the OSP is necessary. "The Tier 2 OSPs are becoming a concern to more and more audit committee members, CFOs and CEOs. For example, consider a law firm. All companies engage law firms, typically multiple ones. SOC reports are not normally going to apply to them because they are not usually performing internal controls over financial reporting on behalf of the client. But yet, there is heavy risk exposure – they are handling intellectual property, they are handling SEC filings, they are handling sensitive case information and litigation. Therefore, there needs to be comfort around these service providers."

Ron Kral, managing partner at Candela Solutions LLC

From a more operational perspective, the financial services industry is heavily focused on OSP risk assessment. "One company's risk profile might be much different from another, but the fundamental starting point is how critical the OSP is to the company's overall process. If the OSP had an outage, how would that outage impact the company's business continuity and the company's ability to transact business?"

Considering the following in assessing the financial risk of the OSP is a good idea: Are they a going concern? Are they compliant with regulatory rules? Do they have reputational risk? "Companies don't want to be associated with unsavory parties. A final important factor is that risk assessment cannot be looked at as a *cookie cutter* approach; risks vary based on the particular OSP."

Chris Ritterbush, executive director at EY's Advisory, Performance Improvement

---

Regulated industries, such as financial services, have generally been focused on OSP risk assessment and management for a longer period of time than other industries. However, these concerns are now top of mind for many organizations across most industries due to the implementation of the *2013 COSO Framework*, and the federal government's National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF), which emphasizes OSP risk management. "From the commercial space, we see a sensitivity to supply chain risk, as they go through this risk assessment – the failure of a key supplier can shut down a production line, or even impair a hospital's ability to deliver care."

Chris Halterman, executive director at EY's Advisory Services

HOW RELIANT ARE USER ORGANIZATIONS ON SOC REPORTS?

Many interviewees felt that SOC[6] reports provided by OSPs are helpful as a starting point; however, they also believe that these reports must be augmented by additional controls and considerations to create a truly effective internal control process. That said, there is more demand for SOC reports by user organizations as they have limited resources.

In the absence of receiving a SOC report, or receiving a report that does not address controls in line with key controls identified by the company, it is suggested that additional controls and procedures need to be in place to mitigate risk.

> Whether or not the OSP had a SOC report, "It is most important to view the OSP as an extension of your company. Ask yourself if these are the key controls necessary to ensure that this information is materially accurate. If you find that these aren't being performed by the OSP, you need to figure out how you can accomplish that control. Whether this may be actually testing the control at the third party or relying upon their [SOC] report –there needs to be a bridge to ensure that we [the organization] are addressing the key controls to ensure accuracy."
>
> ***Senior director of corporate accounting at an electronics manufacturer***

Mitigating controls, in either case, may include: reconciliations, validations of expectations, performing controls over the OSP, and onsite visits of the service providers.

> *On having a SOC report*
>
> "We rely on the SOC reports provided by the service provider. However, on top of this report, we have validations to expectations, pay simulations, and reconciliations. We have a number of controls in place to validate that the information coming from the service provider is accurate. For example, Bank A is the custodian of all our financial investments. Monthly, we prepare what we expect our position (realized and unrealized gains or losses) to be and compare that to the information that Bank A feeds into our general ledger. It is not a dollar for dollar science, but it does allow us to ensure what is being fed into our ledger is accurate. Differences between our calculation and Bank A's are investigated. We provide evidence that this process is performed as part of our key controls."
>
> ***Senior director of corporate accounting at an electronics manufacturer***

[6] For clarification purposes, SOC 1 reports focus on financial reporting risk and controls specified by the service provider and are most applicable when the service provider performs financial transaction processing or supports transaction processing systems. A SOC 2 or 3 report focuses on security, availability, confidentiality, processing integrity ,and privacy. Effectively using SOC 1, SOC 2 and SOC 3 reports for increased assurance over outsourced operations, KPMG, 2012.- https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/SOCWhitepaper.pdf

The SOC reports do not generally contain controls addressing the other four components of the *2013 COSO Framework;* i.e., control environment, risk assessment, information and communication, and monitoring activities. Regardless of the fact that the company obtains a SOC report, one should still consider controls for these components over the OSP. "The company needs to come up with a solution, a response, generally by articulating their controls as per the three tiers using a risk assessment approach to accommodate each of these other components. Therefore, it may be critical to involve the company's internal auditors."

Ron Kral, managing partner at Candela Solutions LLC

Controls are performed above and beyond those of the OSP based on the service that is being provided. "The controls vary considerably, depending upon the service being provided. We do receive a SOC report for many of the financial applications; however, for something like plant operations, we don't get anything that remotely resembles a SOC 1 report. Therefore, a member of our internal operations group has to oversee the work of the OSP within the manufacturing facility. For OSPs that do provide a SOC report, such as a payroll company for our employees, we review the SOC reports. However, we also do have some internal controls over making sure that the data we transmit is received, and we reconcile the summary information back to our other records."

Director of Internal Audit at a chemical manufacturer

"From an operations perspective, our security standards include the ability to audit and layer control points that OSPs would need to provide periodically. If a SOC report is obtained, the controls are minimal but annual revalidations must occur that they have maintained that compliance."

VP of finance and IT transformation for a technology company

Regardless of whether or not a SOC report is provided, OSPs are asked to fill out the questionnaire his company has prepared. "Open communication and an in-depth discussion with the OSP are also critical to determine their security structure. For example, just asking what type of antivirus software they maintain – this normally gives insight into their security structure. If the OSP mentions they are using antivirus software that hasn't been supported in the past 20 years – that throws up red flags."

Network security analyst at a restaurant chain

On not having a SOC report

"If an OSP does not provide a SOC report, it is recommended to either perform tests of the user organization's controls over the activities of the service organization or perform tests of controls at the service organization. Each of these options may be challenging to complete, depending on the nature of the services provided. For example, when testing monitoring activities of the user organization over the OSP, the monitoring activities have to be sufficiently precise, such as testing the user organization's independent re-performance of items processed by the OSP. The ability to directly test controls at the OSP requires a 'Right to Audit' clause in your contract with the OSP as well as sufficient resources, skillsets and time to do the testing."

Sandra Herrygers, Deloitte Advisory partner at Deloitte & Touche LLP

"In the financial services area, there are a lot of organizations that do go out and do the monitoring of the OSP – through either an onsite visit or through a self-assessment. They base the standards on their own internal assessment."

Chris Ritterbush, executive director at EY's Advisory, Performance Improvement

---

On increased reliance over SOC reports

"The demand for SOC reporting is increasing. We continue to see the demand of the SOC 1 growing. But keeping in mind that the SOC 1 is a special purpose report intended to address financial statement risk arising from OSPs, the demand for these reports are fairly mature. With the adoption of [the] *2013 COSO Framework* and the broadening of concerns over internal control[s] relating to operations and compliance, companies are increasingly interested in obtaining a SOC 2 report from their OSPs. In fact, in developing the 2014 revisions to Trust Services principles and criteria (used as the basis for SOC 2 reporting) the AICPA referred to the *COSO 2013 Framework* to understand the internal control of the users of the report. This understanding is reflected in the wording and structure of the criteria."

Chris Halterman, executive director at EY's Advisory Services

"Survey results reveal there has been a significant upswing year over year of companies' reliance on the SOC reports. SOC reports make the picture more robust."

Chris Ritterbush, executive director at EY's Advisory, Performance Improvement

WHAT ARE SOME CHALLENGES COMPANIES ARE FACING WITH INTERNAL CONTROLS OVER OSPS?

The auditors acknowledge there are challenges with internal controls over OSPs. These include a lack of a formal documentation testing of controls over the OSP's code of conduct or ethics programs; ascertaining whether the OSP complies with regulatory requirements; and ensuring that the OSP has adequately addressed cybersecurity.

Most organizations had to formally document and implement controls over OSPs in areas where they didn't have to before. OSP-related controls, which were previously concentrated in the monitoring component of COSO, are now dispersed among the other COSO components. This has resulted in organizations formalizing OSP controls in these additional areas to achieve the related COSO principles. For example, previously, most companies did not formally document and test controls over the OSP's code of conduct or ethics program; nor did they document methods to select and evaluate an OSP for service.

On the other hand, most organizations had existing controls in the monitoring component in place for years prior to the *2013 COSO Framework*. Almost all companies had a monitoring process where they would obtain a SOC report for OSPs providing services relevant for their ICFR. This process typically included evaluating qualifications and/or exceptions noted in the report and also testing their own end-user control considerations listed in the report.

Sandra Herrygers, Deloitte Advisory partner at Deloitte & Touche LLP

From a financial services perspective, one of the main considerations is the OSP's compliance with current regulations. "If a regulator does come in and evaluates an important systemic vendor and if found that they are not compliant with regulatory issues, the company will be held responsible."

Chris Ritterbush, executive director at EY's Advisory, Performance Improvement

---

In the past 18 months, the publication of the NIST CSF has brought attention to the fact that organizations have not sufficiently assessed cybersecurity risks and implemented sufficient controls and mitigation strategies to address those risks that needed improvement. "The cybersecurity vulnerabilities may result in the failure of a manufacturing process or the lack of availability of goods and services."

Chris Halterman, executive director at EY's Advisory Services

How are auditors getting comfortable with an organization's controls around OSP?

Once controls of the OSPs have been identified (either through SOC reports or otherwise) and documented, it is necessary for the company to obtain evidence that these controls over the function of the OSP are effective. Documentation of testing the controls of the company and/or the OSP or obtaining a SOC report are various ways to provide evidence that controls are effective.

> "An important consideration in evaluating controls is the nature of the services provided by the OSP as these are not all created equally. The more significant the risk around the services provided by the OSP, the more persuasive the corresponding audit evidence has to be. Varying the nature, timing, and extent of testing based on risk is really important from an auditor judgment perspective. For example, auditor expectations of controls over a routine payroll OSP are generally much less extensive than expectations of an OSP providing services related to an account which is based on a significant judgment or estimate. Auditors also specifically consider how the user organization's management monitors the activities performed by the OSP, and/or how they control the data interfaces between the user organization and the OSP."
>
> ***Sandra Herrygers, Deloitte Advisory partner at Deloitte & Touche LLP***

> "In understanding an OSP and its controls, we view things from the financial statement assertion perspective. In a financial audit, we focus on the controls at the OSP, over the input that is sent to it, how that input is processed and the output received back from [the] OSP, particularly looking at the SOC 1 report to understand what the OSP actually does. We also understand what controls the OSP expected to be implemented at the user entity – or the company going through the financial audit, and perform procedures to determine if those controls are in place. Usually these 'controls expected to be in place at the user entity" are transactional controls that are a routine part of processing, but often they do identify key monitoring controls that are important to overseeing the processing of the OSP. This is the bottom-up approach to OSPs in a financial audit. Increasingly, we also consider the impact of OSPs from the top down. In these situations, we are not only looking at the general risk management or the user entity but also their vendor risk management program, looking more broadly at what the organization is doing to address these risks."
>
> ***Chris Halterman, executive director at EY's Advisory Services***

WHAT GUIDANCE ON CONTROLS OVER OSPS CAN YOU PROVIDE SENIOR-LEVEL FINANCIAL EXECUTIVES?

Our interviewees provided recommendations concerning controls over OSPs. These include: an OSP's risk assessment should not be a *one-size-fits-all* solution; organizations need to be nimble and contemplate risks through monitoring and initiating remedial measures to mitigate these risks; companies need to assess the financial viability of the OSP and take a deep dive into the SOC report by reviewing and understanding it; and other functional areas need to be involved with the selection process of an OSP; otherwise there may be overreliance on the OSP by a concentrated group in the user organization.

"Don't treat OSPs as a *one-size-fits all*; vary the nature, timing and extent of your procedures based on risk. For ICFR, applying a risk-based approach is key because focusing on the areas with the highest risk helps protect investor confidence in the capital markets."

Sandra Herrygers, Deloitte Advisory partner at Deloitte & Touche LLP

"What is important for companies is to contemplate risk and then monitor, manage and remediate to the significance of the 'targeted' risk."

Chris Ritterbush, executive director at EY's Advisory, Performance Improvement

---

As practical guidance, it is suggested that senior-level financial executives need to get a handle on the objectives, risks and controls on those activities outsourced to a service provider. And, while the usage of OSPs is increasing, this does not relieve management from responsibility for OSP controls Finally, strict reliance on SOC reports is not enough. It's important to apply additional procedures, including these three commonsense ones:

1. Verify that the scope of the audit work from the service provider covers your services.
2. Verify that the firm signing the AICPA report (i.e., the SOC-1 reports) is an active licensed CPA firm or sole practitioner.
3. Be aware of the noted deficiencies in the SOC reports, and especially management response. Follow up with management of the OSP to ensure the proper corrective actions are occurring.

Ron Kral, managing partner at Candela Solutions LLC

A suggestion directed to SOC reports: "Don't just stop at obtaining a SOC report, read it and understand the controls that are in place there, making sure that the tests have been performed, understanding the results of the test and then performing additional steps to get comfortable with the information as it comes in. I see that a failure in a key control at the OSP is the same thing as a failure of the key controls for your organization – this may cast doubt on that OSP. The challenge becomes integrating these SOC reports in an organization's control system – this was the root of many companies' failure to adequately comply with SOX."

Senior director of corporate accounting at an electronics manufacturer

"I have a few suggestions for senior-level financial executives. Firstly, get the procurement group involved as another set of internally independent eyes. We had an incident where the 'financial' group had run the selection of a vendor – which was a problem once we identified it. Make sure the functional guys aren't too close to the vendor. A second suggestion stems from an observation -- once a function outsources a task to an OSP, they tend to forget about it. Hence, constant reminder is necessary that management is still responsible. As remediation, we have requested that employees do a periodic formal evaluation of the service provider. Another forewarning is to be alert [to] OSPs who outsource to lower-level OSPs – this may be an additional layer of risk that should be considered by the company. A solution may be to double-check contracts with OSPs to determine if there is a contract within a contract; if so, this must be highlighted to prevent this scenario."

Director of internal audit of a chemical manufacturer

"It is important to adopt security around OSPs and information that is transferred back and forth. For example, having a security standard on what we do is very important. It provides a few ways to close contracts, offers a framework and model, and it also gives guidance to the vendors -- what targets they have to hit for the company to sign an agreement with them -- which they appreciate."

VP of finance and IT transformation for a technology company

"I strongly recommend verifying backgrounds, also hiring people who are technically skilled and think like a criminal. If they don't think about it like how a criminal would, then somebody can subvert a control and get what they want."

Network security analyst at a restaurant chain

We provide a checklist of items to consider when contemplating control over OSPs.

a. Outsourcing must follow existing policies, such as those governing purchasing and information technology. All suppliers are expected to follow an established Code of Ethics published specifically for vendors, reference to which should be included in the contract.

b. The purchasing function must ensure the OSP contract contains clear definitions of control requirements and assurance commitments (e.g., SOC report, Right to Audit clause, etc.)

c. The contracting function is responsible for managing risk and risk mitigation (controls). Responsibility cannot be outsourced.

d. Risk assessment starts during the vendor selection process, in which control requirements should be included in the Request for Proposal process.

e. The current controls should be designed and modified for the new outsourced environment, so the resulting combination is effective. The level of risk to the company should not increase without appropriate thought and approval.

f. Outsourcing removes a process from the company's control environment; therefore, some controls provided by other functions must be explicitly identified and created in the new process (for example, management ethics monitoring or established network security).

g. Controls at the service provider must be monitored to ensure they are effective over time. The company should modify its own controls (as noted above) to compensate for any weaknesses in the controls of the service provider.

Members of the Internal Control Compliance team at a chemical company

INTERVIEWEES' BIOS

FERF would like to offer a special thank you to the following individuals for their participation in this project:

- **Chris K. Halterman**, executive director in the Advisory Services practice of Ernst & Young LLP, with more than 26 years of experience in the public accounting profession with a focus on IT and process controls and information integrity. He leads E&Y's Advisory Service Organization Control Reporting practice globally and in the Americas, with responsibility for developing methodology, training, client service strategy, quality assurance programs and market initiatives. Chris also chairs the AICPA Trust/Data Integrity Task Force.

- **Sandra Herrygers**, Audit and Enterprise Risk Services (AERS) IT Specialist Group at Deloitte & Touche LLP. In this role, she oversees the quality of IT audit services, including functioning as a consultation resource for IT- and internal-control-related matters on the largest and most complex integrated audits. Further, she leads development of approaches, tools, practice aids and learning for IT specialists. For the past year, Sandy has been providing thought leadership and assisting clients and engagement teams in implementing the *2013 COSO Framework*.

- **Ron Kral**, managing partner of Candela Solutions LLC, a public accounting firm with a national focus on governance, compliance and internal auditing. He is an educator, advisor, and internal auditor for boards and management teams, especially for public companies registered with the SEC. Ron has worked with over 200 clients as a Public Accountant, many through Big 4 firms. He brings practical expertise on regulations, accounting and auditing to the table for holistic solutions. He served on FEI's working group for the development of the *2013 COSO Framework*. Currently, Ron serves on FERF's Research Committee and the working group for COSO's updated ERM Framework.

- **Christopher M. Ritterbush**, executive director, Advisory, Performance Improvement of Ernst & Young LLP. Chris leads the global supplier assurance service offering and has extensive experience delivering engagements for peer financial-services clients for over 10 years.
  Chris has designed and deployed supplier risk programs for some of the largest leading financial institutions. Chris is also active in industry groups designed to improve supplier risk management practices.

In addition to the interviewees listed above, other executives from companies engaged in chemical manufacturing, restaurant retail, technology, and electronics manufacturing were interviewed. For privacy reasons, these individuals did not wish to be quoted directly and asked to remain anonymous. Their titles include director of internal audit, members of Internal Control Compliance team, vice president of finance and IT and network security.

About RR Donnelley

RR Donnelley provides the technology and expertise so companies can create, manage and deliver accurate and timely financial communications. We file 160,000 client submissions annually with the SEC and produce critical documents for regulatory compliance and business transactions. As a Fortune 500 company with a 150-year history, our 65,000 employees deliver solutions to 60,000 clients across all industries and stages of development in 37 countries – all to produce and distribute documents and electronic communications for shareholders, regulators, and investors.

ActiveDisclosure: Expert-Supported Online Compliance Filing:

Providing finance, legal, and investor relations professionals with greater control and enhanced flexibility, ActiveDisclosure delivers increased efficiency, stronger governance, and the highest quality financial reports. Our experts are available 24/7 to help personally guide you through the financial reporting process, maintaining the highest level of security and confidentiality throughout. ActiveDisclosure is the first reporting solution in the industry to be SOC 2 Type II certified.

Mitigating risk while delivering best-in-class solutions and services is always our top priority. When you choose RR Donnelley ActiveDisclosure, you'll know that your business and data are safe, secure and protected by the strongest safeguards and controls in the industry.

For more information:

Our team of experts is always willing to furnish further information about what we're doing to provide you with the peace of mind you need to focus on your business. For further details, please contact your local sales representative or call us at 800-424-9001.

About Financial Executives Research Foundation

Financial Executives Research Foundation (FERF) is the non-profit 501(c)(3) research affiliate of Financial Executives International (FEI). FERF researchers identify key financial issues and develop impartial, timely research reports for FEI members and non-members alike, in a variety of publication formats. FERF relies primarily on voluntary tax-deductible contributions from corporations and individuals. Questions about FERF can be directed to bsinnett@financialexecutives.org. The views set forth in this publication are those of the author and do not necessarily represent those of the FERF Board as a whole, individual trustees, employees, or the members of the Research Committee. FERF shall be held harmless against any claims, demands, suits, damages, injuries, costs, or expenses of any kind or nature whatsoever except such liabilities as may result solely from misconduct or improper performance by the Foundation or any of its representatives. FERF publications can be ordered by logging onto www.ferf.org.

International Standard Book Number

978-1-61509-187-4

Printed in the United States of America

First Printing

Financial Executives Research Foundation (FERF) gratefully acknowledges these companies for their longstanding support and generosity

PLATINUM MAJOR GIFT | $50,000 +

Exxon Mobil Corporation
Microsoft Corporation

GOLD PRESIDENT'S CIRCLE | $10,000 - $14,999

Cisco Systems, Inc.
Cummins Inc
Dow Chemical Company
General Electric Co
Wells Fargo & Company

SILVER PRESIDENT'S CIRCLE | $5,000 - $9,999

Apple, Inc.
The Boeing Company
Comcast Corporation
Corning Incorporated
Credit Suisse AG
Dell, Inc.
DuPont
Eli Lilly and Company
GM Foundation
Halliburton Company
The Hershey Company
IBM Corporation
Johnson & Johnson
Lockheed Martin Corp.
McDonald's Corporation
Medtronic, Inc.
MetLife
Motorola Solutions, Inc.
PepsiCo, Inc.
Pfizer Inc.
Procter & Gamble Co.
Tenneco
Tyco International Mgmnt Co.
Wal-Mart Stores, Inc.

GOLD CORPORATE LEADERSHIP - $2,500 - $4,999

Aetna, Inc
Accenture LLP
Intel Corporation
Raytheon, Inc.
Select Medical Corp.
Time Warner, Inc.
United Technologies Corporation
The Walt Disney Company

SILVER CORPORATE LEADERSHIP - $1,000 - $2,499

American Financial Group, Inc.
Barnes Group, Inc.
Edward Jones
Graham Holdings
The J.M. Smucker Company
McCormick & Company, Inc.
OMNOVA Solutions, Inc.
Paychex
Scripps Networks Interactive, Inc.
Telephone and Data Systems, Inc.
Trinity Industries, Inc.