Greetings to my fellow Customer-Supplier Division members!

Many of us have probably heard the old adage that the only thing constant in life is change. If you have been reading recent communications from ASQ, you’ve probably learned about ASQ’s transformation initiative. It is meant to ensure that ASQ is positioned to continue to provide value to its members for the foreseeable future.

The transformation efforts touch on every part of ASQ, including all of the Divisions. ASQ’s Board of Directors and the Technical Communities Council (TCC) are working with the Divisions and other Technical Communities to develop and implement new management structures and financial systems. What isn’t changing is the overarching purpose of the Divisions, which is to provide technical expertise to our communities and to continually expand our bodies of knowledge.

The leadership team of the Customer-Supplier Division is working diligently with the Board and the TCC on the transformation initiatives. Rest assured, regardless of the changes to our management structure, we will continue to develop new technical content for you, through our publications, training courses, webinars, conference sessions, and this newsletter.

No matter what, CSD will continue to fulfill its mission to you:

To provide answers that develop, improve, and strengthen customer-supplier relationships.

Best regards,
Stephanie Parker
Chair, Customer-Supplier Division
Happy Spring!

As the new editor, I welcome you to our first edition in 2019. I am so excited and grateful for the opportunity to serve you in this capacity.

This edition spotlights the issue of third party GDPR risk. This risk is inevitably due to the higher data processing activities of present-day companies, large and small. This edition also shares a best practices risk management program. We are in the quality business and our customers are our lifeline. In our various businesses, we have customers to satisfy as well as suppliers we have to rely on, and they affect the success of our companies. As the saying goes: “The height of a tree is the depth of its roots”. Incorporating these best practices might be prudent. Let’s go for it.

I would love to hear from you regarding any feedback you may have on the newsletter as well as possible topics you wish to see included. If you have articles that have been previously published and presented, or if you simply enjoy writing, we will be very happy to share your work with the readership. Perhaps you have a customer success story or a not-so-successful story that you learned from, let’s share our knowledge with everyone, learn from each other, and ensure quality remains at the top. Please contact me at habibo@coned.com.

The World Conference on Quality and Improvement (WCQI) is around the corner. Please make every effort to attend. We expect plenty of fun and learning opportunities at the Conference.

Thank you for your readership and dedication to our Division. I hope you enjoy the articles. See you at the WCQI in Fort Worth, Texas.

Sincerely,
Olabisi Habib
Editor, Customer-Supplier Division
What Is Vendor Risk Management?

It wasn’t long ago—perhaps just five or ten years—that your company viewed third-party vendors as merely providers of goods and services to your business. The conventional wisdom back then characterized vendors (including consultants and contractors) as suppliers, not business partners; so their problems weren’t your problems.

But that was then and this is now. Several influences have forced a change in how you look at vendors and the risks they might pose to your business.

Globalization has created a dependence on critical activities outsourced to an increasing number of partners and vendors; this in turn has fueled a dramatic rise in the third-party ecosystem. It’s highly likely that your company now outsources significant aspects of its business to outside providers. Whether it’s accepting orders over the Web, manufacturing various products or components, or delivering services across town or to far-flung markets, your company relies on other companies to fill important needs of one sort or another. In effect, this makes them extensions of your own company. What’s more, in this age of globalization, your critical suppliers can be anywhere in the world, including “in the cloud.”

Having a dependency on outsiders increases your company’s vendor-related risk. Oftentimes, your vendors are provided access to your intellectual property or to sensitive customer information. With significant security compromises making headlines, it’s no surprise that most organizations are now requiring vendors to abide by not only their internal standards, but also by industry and governmental regulations surrounding privacy and security.

This heightened regulatory environment is a major influence, designed to force companies like yours to assess and address internal and external risks. It is an
effort to maintain stability and to protect customers and investors alike. Regulations such as Basel II, Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the Health Information Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and Federal Financial Institutions Examination Council (FFIEC) guidelines, among others, mandate that risk-management policies extend to third-party vendors, outsourcers, contractors and consultants. Third (and fourth) parties have the potential to insert risk into your environment because they are outside your direct sphere of control.

Good corporate governance—which can't be legislated-means you have an obligation to understand vendor risk and to actively take steps to mitigate the risk and its impact on your business. Simply put, you need a single, collective view of your vendor risk in order to manage it well and have a more stable and productive business ecosystem.

Why Assess Vendor Risk Management?

For most companies, regulatory requirements are the leading reason to conduct vendor risk management (VRM) assessments. External regulators as well as internal auditors are expecting that you thoroughly understand the range of risks inherent in doing business with outside organizations, and that you have taken measures to lessen the impact of those risks on your own business. Regulatory compliance is well and good, but there are additional motivations to assess third-party risk. One reason is to protect your company’s brand and reputation from being damaged by another company’s actions. Consider how Wal-Mart’s reputation was tainted when 112 people died in a fire at a Bangladesh clothing factory in November 2012. The company that owned the factory, Tazreen, was an unauthorized supplier to Wal-Mart’s official clothing vendor. Apparel bearing Wal-Mart’s Faded Glory label were found in the rubble. While Wal-Mart claimed it didn’t know Tazreen was manufacturing its clothing, the Wall Street Journal and other news media associated the global retailer with dangerous working conditions in developing countries.

The more deeply you understand your partners’ ways of business, the easier it will be for you to maintain quality of service (QoS). This includes both the level of service to you from your vendors, and to your customers from your company, especially when your vendors touch your customers directly; for example, contract personnel who provide delivery and installation on your behalf. Could their behavior reflect poorly on your company? You bet, because customers often don’t see the distinction between your company and your contracted service providers.

What Is A Vendor Risk Management Program?

A vendor risk management program is a formal way to evaluate, track and measure third-party risk; to assess its impact on all aspects of your business; and to develop compensating controls or other forms of mitigation to lessen the impact on your business if something should happen. A program of this nature

Looking Further Up The Supply Line

When we talk about third-party risk, we mean the companies that you do business with directly. But those companies also have vendors that become fourth parties to you, and they, too, can pose a potential risk. For example, you may have a partner whose IT systems are hosted in the cloud with a fourth party. This is becoming increasingly common. You need to understand how well-protected that cloud environment is. There could be yet another business hosted on that same cloud that is a major target for cyber attacks. A sustained attack could knock your vendor’s business offline for a period of time.

How would your company be impacted if your partner’s IT systems are down?

What measures can you take to mitigate that risk?
gives you consistency for managing your vendors and a way to share information about them within your organization. Whether your VRM program is manual or automated, homegrown or offtheshelf, the important thing is that it reflects and enforces your internal controls framework, ensures your compliance with government or industry regulations, and achieves consistency with all of your vendors.

01. Identify potential vendor risks

Many companies that implement a VRM program wrongly assume they have to deeply assess every business partner. In fact, doing so can be a waste of time and money. Of the hundreds or even thousands of vendors you work with, only a small percentage may present a serious risk to your business, and these are the ones to evaluate thoroughly.

Some of your vendors deserve far more scrutiny than others because of the strategic role they play in your company’s ability to generate revenue from your goods and services. Others may provide a minor service but have the potential to expose confidential information. Therefore, you want to categorize and prioritize your vendors and then focus your assessments on the risks that are germane to specific vendors and the services they provide. Consider which aspects of your business a vendor touches. IT systems? Critical or sensitive data? Business processes? Facilities? Manufacturing? What are your concerns in this area? What is your regulatory exposure? Is this a strategic vendor or a bit player?

For example, suppose you contract a company to accept electronic payments over the Web. This is a high-value partner as it collects revenue for your company and presents your brand to the world. This company touches your customers’ highly sensitive credit card data. A breach of this data could be a financial and public relations nightmare for your company—even if you aren’t directly responsible for the breach. Your risk assessment must include what measures the company has in place to secure this data. Furthermore, this company’s Web applications might be hosted on yet another service provider’s computer systems, dictating the need to expand your risk assessment to this fourth-party company.

Identifying when to assess a vendor is also key. When you start the assessment process early in the relationship, it will help to dismiss any company that has “issues” before you engage in a contractual relationship. For vendors with whom you currently do business, a suggested time to assess them would be prior to renewing the contracts. This will ensure you have time to engage with the vendor and ascertain that control and reliability are adequate for the services they are providing.

02. Develop effective strategies for addressing higher risk vendors

When you have a vendor that your VRM process has identified as presenting substantial risk and you are willing to accept this vendor as a business partner, you need...
strategies to work with the company in order to keep the vendor’s issues from causing you harm. In order to effectively do so, you must consider the following:

• Know what aspect of your business you are trying to protect and focus on minimizing the risk in that area. Make risk mitigation part of the negotiation and contract service-level agreement (SLA).

• Work closely with the vendor to identify and resolve issues to lessen your risk.

• Assess the vendor prior to contract renewal or more frequently; conduct ad hoc reviews when concerns arise.

• Gather outside information about the vendor, such as from Moody’s or Dun & Bradstreet, to assess financial health. These services might advise you of issues that are affecting your partner’s performance.

• Use metrics to measure the vendor’s performance over the time of your relationship. This can show if the partner’s service level is improving, holding steady or declining.

• Have a plan of what to do if a vendor exceeds your threshold for risk. You also should have plans for all vendors in the event they are put out of business for any reason, such as an act of nature or financial collapse.

03. Align vendor control environments with your internal framework

Your company already has a control environment to mitigate your internal risks—likely based on ISO, NIST, or PCI control sets or reflecting the COSO or COBIT risk/process frameworks. Now you must work with your vendor to assess the effectiveness of controls it has in place for the risks you’ve identified with that company. Realize that you can’t get the same level of detail from a vendor as you do from your internal groups.

However, some service providers, including cloud service providers, will have an SSAE 16 SOC report, which provides a control benchmark to use when comparing outsourced service providers. Should your vendor not have an SOC report, your organization can stipulate the need for audits in your vendor agreement.

Regardless of how you gain insight into a vendor’s internal control systems, you should perform a gap analysis of your controls versus the vendor’s controls, and work together to close the gap and align the vendor’s controls to your specific needs. These needs should be aligned with industry control standards and guidelines.

When determining vendor internal control requirements, you should recognize that no single standard or guideline is appropriate for every organization. A best practice is to identify services and capabilities of the vendor and map them to the relevant industry regulations and control standards. This effort can be helpful in meeting compliance goals.

04. Implement ongoing oversight utilizing metrics and external alerts

Once you’ve identified your key vendor risks, metrics are a way to measure actual performance against those risks. Set up metric exception levels and what risks are tied to it. For example, suppose you have a business process that relies heavily on contract workers. You expect some level of worker turnover, but lately the turnover rate has become excessively high. The exodus of workers not only affects your productivity, but it also exposes you to higher training costs for replacement workers and leads to a potential for data breaches by ex-workers who still have system access.

External alert services also can clue you in to potential problems, such as when a key vendor has an issue that may impact your business. Say your vendor is being acquired, or a major lawsuit has been filed against the company. An early alert gives you the opportunity to meet with your partner sooner rather than later to discuss the issue and develop a plan to minimize your risk.

When developing measurements, it’s important to identify the business value that is intended to be gained with the function or capability being measured, and then define objective criteria that can be used to assess this value. This is important because subjective measures can be open to interpretation by the audience evaluating the metric. Some measures to consider include:
Processunity & Vendor Risk Management

ProcessUnity is a leading provider of cloud-based applications for risk management and service delivery management. The company’s software-as-a-service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes. ProcessUnity’s cloud-based Vendor Risk Management solution helps companies effectively identify and mitigate risks posed by third-party service providers in critical risk areas such as information security, service delivery, supply chain processing, financial processing, reputation, and regulatory compliance. ProcessUnity provides organizations with clear visibility into the business impact of third-party risk via direct links from vendors and their services to specific business elements such as processes and lines of business. Powerful assessment tools enable evaluation of vendor performance based on customer-defined criteria through automated, questionnaire-based self-assessments as well as through detailed audits of vendor controls. Flexible reports and dashboards enable ongoing monitoring of vendor ratings, assessment progress, and status of remediation activity. Learn more at http://www.processunity.com.

Your Next Steps

Vendors provide value in the expertise and services they offer; however, it is imperative that companies maintain active oversight. As a manager of business risk, you must recognize that when a vendor performs a service or function on your behalf, your company bears the ultimate responsibility for minimizing business exposure and ensuring compliance.

Because varying levels of risk remain with the company that offers the product or service, a strong and comprehensive automated VRM program is necessary to truly understand and track the risks your vendors pose to your business interests. Once you thoroughly understand, measure and track your risks, you can develop strategies to mitigate them to protect your company from harm. With effective vendor risk management, your company can minimize the risk of less direct oversight or control and maximize the benefits gained through a well-managed vendor relationship.

- Performance and SLA expectations
- Disruption in workflow based on vendor performance
- Expectation or vendor-issued warning that workflow may be disrupted for any reason
- Breach of the vendor network, systems or facilities
- Information/results on tests of internal security (physical or systems) controls
- Vendor (non) compliance with laws, rules, regulations, policies and procedures
An action plan for tackling third-party GDPR risk

The European Union’s General Data Protection Regulation (GDPR) has significantly increased the risk of outsourcing data-processing activities of business operations involving European individuals.

The GDPR expands the breadth and depth of third-party risk for large multinationals, which often engage thousands of vendors that perform some type of processing of EU personal data. These companies need an action plan and ongoing capability to mitigate the GDPR enforcement and litigation risk of their supply chain.

Broader and deeper vendor GDPR risk

Five articles in the GDPR add new requirements or deepen existing obligations from the legacy 1995 EU Directive on Data Protection:

• Article 28, “Processor,” requires contractual protections with data processors and their sub-processors, adequate data protection, and production of evidence of compliance with the GDPR;

• Article 30, “Records of processing activities,” requires data processors to maintain a detailed inventory of the EU personal data they host;

• Article 32, “Security of processing,” requires data processors and their sub-processors to implement comprehensive information security controls to protect EU personal data;

• Article 33, “Notification of a personal data breach to the supervisory authority,” requires data processors to report compromises of EU personal data to their clients without undue delay; and

About the article

To discuss further, please contact:

T.R. Kane, Global Third Party Risk Leader  
+1 (440) 390 8502 
t.kane@pwc.com

Jay Cline, U.S. Privacy Leader  
+1 (763) 498 2237 
jay.cline@pwc.com

Contributors: Justin Hall, Andrew Namoury, Nikhil Sarnot, Nehal Sheth, Michael Spadea and Dean Spitzer

pwc.com/us/gdpr

© 2018 PwC. All rights reserved. PwC refers to the U.S. member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate entity. Please see www.pwc.com/structure for further details.
• Article 36, "Prior consultation," requires data processors to provide data protection impact assessments (DPIAs) to their clients in certain high-risk situations.

Companies which engage third parties to process their EU personal data will also want to contractually establish their service levels for assisting with responses to data subject rights requests under their purview and also to provide GDPR evidence of compliance on demand.

Enhancing existing third-party risk-management programs to address GDPR

Most multinationals already operate a third-party risk-management (TPRM) program to address their vendors’ information security risks. These programs often involve maintaining an inventory of third parties and the type of data they process; requiring vendors to adopt standard contractual clauses addressing information security; and vetting vendor responses to security due diligence questionnaires. A growing number also include on-site security reviews or audits in their programs.

To address GDPR vendor requirements, companies doing business in Europe should consider launching an action plan that enhances their existing TPRM program with the following components:

• Adding several columns of GDPR-related metadata to their vendor data inventory
• Adding new GDPR-related criteria to the vendor risk-ranking formulas
• Adding privacy-related requirements to the standard contractual clauses and rolling those addendums out to impacted third parties
• Adding privacy-related requirements to due diligence questionnaires
• Adding privacy controls to onsite audits
• Enhancing the frequency and rigor of ongoing vendor monitoring to detect changes in the scope of vendors’ data processing and facilitate reporting of DPIAs and suspected compromises of EU personal data

Expanding the scope of data protection due diligence

After reviewing GDPR requirements, it seems that the EU expects organizations to conduct a greater level of due diligence on their third-party relationships. Organizations must understand the nature, scope, context, scale and purposes of processing as it relates to services performed by third-parties in order to establish an appropriate level of oversight. One solution is to leverage a modified due diligence assessment which incorporates requirements from DPIAs. This assessment not only supports the EU’s objective of more stringent oversight for third-parties that are handling data subject’s information, but it also helps identify processes that may result in a high risk to the rights and freedoms of natural persons, as defined by GDPR’s Article 35:

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.”
In collaboration with its Data Privacy Officer (DPO) or appointed privacy leader, a firm should consider expanding its due diligence assessments to contain at a minimum the following: (1) a systematic description of the envisioned processing operations; (2) the purposes of the processing; (3) as applicable, the legitimate interest pursued by the controller; (4) an assessment of the business necessity need to perform the services; (5) an assessment of the risks to the rights and freedoms of the data subjects; (6) the measures envisioned to address the risks including safeguards and security measures; and (7) mechanisms to ensure the protection of personal data and to demonstrate compliance.

Under GDPR, all third parties (processors) handling data jointly (i.e., joint-controllers) or on behalf of another firm (i.e., controller) will be required to meet new requirements. If these requirements are not met, the controller and or the contracted third parties will be held liable, resulting in potential fines, sanctions and brand impact. Therefore, it is important for organizations to update the due diligence process to consider these privacy requirements:

- Third-party breach notifications
- Records of processing
- Roles and responsibilities
- Security controls
- Doing business across borders
- Demonstrating compliance

When should a firm perform the modified due diligence assessment?

It is common practice for organizations to conduct assessments in high-risk situations, but when dealing with personnel data, organizations should consider taking a more strategic approach which considers unconventional processing activities, technologies and scope of services. Although organizations have the ultimate decision as to when due diligence assessments should be performed, it is important to evaluate all third parties that may impact the rights and freedoms of natural persons. Unfortunately, an exhaustive list of processes or activities that would require an assessment does not exist. But GDPR has provided some basic guidance and sample scenarios for consideration. The guidance includes but is not limited to the following:

- A third party is, or will be, performing a high-risk process or services which may impact the rights and freedoms of natural persons
- A third party is, or will be, systematically monitoring a large scale publically accessible area
- As referenced in Article 9(1), any third-party processing special categories of data on a large scale and/or personal data containing criminal convictions or offense
- A third party is, or will be, evaluating personal aspects relating to natural persons based on automatic processing, including profiling, and on which decisions are based that produce legal effects concerning the natural persons
- A third party is, or will be, leveraging new technologies, or those of a type in which no data protection impact assessment has yet been carried out
- A third party is, or will be, performing additional processing activities which require the completion of a DPIA as defined by the supervisory authority

Additional processing activities and businesses to consider:

- Consumer facing activities
- Activities relating to children
- Marketing and advertising
- Digital transformation
- Geolocation
- Profiling
- Tracking
- Public services
- Mass communications
- Joint ventures
- Global business operations
Time to update those contracts

Organizations now have a legal obligation to establish contractual agreements between controllers and processors which clearly define the roles, responsibilities and liabilities of both parties. The goal of each contract at a minimum should include:

- The subject-matter and duration of processing
- The nature and purpose of processing
- The type of personal data and categories of data subjects
- The minimum terms or clauses required of the processor
- The obligations and rights of the controller

This new requirement ensures that organizations not only comply with GDPR requirements, but it also ensures that controllers and processors provide appropriate protection over data subjects and their personal data.

Continue to improve ongoing monitoring

The harsh reality under GDPR is that organizations and their third parties are under more scrutiny to monitor and maintain compliance as referenced in Articles 28, 31, 32(d) and 39. Not only will third parties need to cooperate with the supervisory authority, but they will be expected to establish methods for determining the effectiveness of technical and organization measures. Such methods may include risk assessments, high-risk processes, the type of data and how it’s being processed and the number of active processors.

The new regulation also states that DPOs or appointed privacy leaders who are aligned to a controller or third-party processor are expected to monitor a firm’s compliance with GDPR and other applicable provisions as determined by EU member states. Therefore, ongoing monitoring activities, processes and measures should be evaluated and updated as part of “business as usual” operations. And because third-party relationships may evolve over time, organizations need to be flexible and adapt their strategies to effectively manage changes in the level and types of risks associated with each relationship.

Termination of third-party relationships

Although GDPR doesn’t provide specific requirements around terminating a third-party relationship, organizations should still plan accordingly for this situation. One option is for organizations to develop a plan for bringing a service in-house or alternatively, finding a replacement third-party provider. No matter which option is chosen, each plan may vary based on each third party or the type of services being provided, and may include, but not be limited, to the following factors: (1) transition timelines, (2) technology and security requirements, (3) data retention and destruction activities (4) legal and regulatory requirements, (5) capability and resourcing needs, (6) impacts to services or business functions and or (7) strategic risks.

In conclusion

Implementation of GDPR will be time-consuming and complex, and will likely cause disruptions throughout the business unless organizations can adopt new strategies to manage the regulatory requirements internally and against contracted third-parties. The most successful organizations may be those which incorporate risk management practices that meet the new enhanced regulations – in a way that allows the organization to also meet defined business initiatives and objectives.
Supplier Quality Professional (SQP) Courses

The Customer-Supplier Division is excited to announce the completion of our redesigned training courses. Whether you’re starting your career as a supplier quality professional or ready to certify, we have the courses you need to advance your career.

Our Supplier Quality Professional: An Introduction course is available as a full series or individual modules.

The Certified Supplier Quality Professional (CSQP) Certification Preparation class is available face-to-face or virtually.

For more information, check out our courses online:

- Supplier Quality Professional: An Introduction – SQP 5 day course
  asq.org/training/supplier-quality-professional-an-introduction-sqp2018asq
- Introduction to Supplier Management – SQP Module 1
  asq.org/training/introduction-to-supplier-management-ism2018asq
- Auditing for Improved Supplier Performance – SQP Module 2
  asq.org/training/auditing-for-improved-supplier-performance-aisp2018asq
- Quality/Engineering Tools for Supplier Management – SQP Module 3
  asq.org/training/qualityengineering-tools-for-supplier-management-qetsm2018asq
- CSQP Certification Preparation – Classroom
  asq.org/training/certified-supplier-quality-professional-certification-preparation-csqpasq
- CSQP Certification Preparation – Virtual
  asq.org/training/certified-supplier-quality-professional-certification-preparation-vcsqpasq

If you are planning to attend the World Conference on Quality and Improvement in Fort Worth, we invite you to join CSD during our business meeting on Sunday, May 19, at 2:00 p.m. in the Omni Fort Worth. During the conference, CSD is sponsoring Session T13, Preparing for Successful Data Integrity Audits, presented on May 21 at 9:15 a.m. by Mary Chris Easterly. Also, be sure to come by Booth #340 in the exhibit hall to meet CSD’s leadership team and let us know what’s on your mind regarding customer-supplier relationships!