A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance

Process guidelines and a framework for boards of directors and senior management must be considered when providing oversight, examination and risk management of third-party business relationships in the areas of information technology, systems and cyber security.

It is hard to find any enterprise that does not rely on third parties to support its operations. Senior management and the board of directors are ultimately responsible for the risk that third-party vendors, contractors and systems impose on the enterprise.

Third parties include, but are not limited to, technology service providers; payroll services; accounting firms; invoicing and collection agencies; benefits management companies; and consulting, design and manufacturing companies. Most third-party commercial relationships require sending and receiving information, access to the enterprise network and systems, and using the enterprise's computing resources. The risk posed at different levels and the impacts range from low to very significant.

Outsourcing an activity to an outside entity is by no means removing the responsibility, obligation or liability from the enterprise, but these activities are considered integral and inherent to operations. As a result, the enterprise is obliged to identify and mitigate the risk imposed on it by third-party commercial relationships.

The number of security breaches and incidents that are the result of third parties is rising. Based on PricewaterhouseCoopers (PwC's) Global State of Information Security surveys from 2010, 2011 and 2012, the number of security incidents attributed to partners and vendors increased from 20 percent in 2010 to 28 percent in 2012.[1] The problem is worsening as the number of enterprises relying on third-party vendors and contractors is on the rise.

Soha System's Third Party Advisory Group surveyed information technology and security managers, directors and executives and found that "with 63 percent of all data breaches linked directly or indirectly to third-party access, those contractors and suppliers who need to get access to corporate applications in order to get their job done represent risk to any enterprise."[2]

The issue of third-party risk is greatly complicated for global enterprises by the sheer number of third parties and contractors that they use to supplement staff requirements and/or services.

The pressure is increasing on global, national, and large or small enterprises to plan, perform, remediate, monitor and report the results of the risk assessment, degree of risk and compliance (regulatory or nonregulatory) that third-party vendors may impose.

Information systems enterprises grant third parties access to company applications, network infrastructure and data centers. However, the senior management team needs to be aware of the severity of such invasive activities to weigh the associated risk factors and to ensure that appropriate procedures are put in place to counter and mitigate the risk.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2fQRcuH

Robert Putrus, CISM, CFE, CMC, PE, PMP
Is a principal with The Roberts Company LLC *(www.therobertsglobal.com)*. He has 25 years of experience in program management, compliance services, information systems and management of professional service organizations. Experienced in the deployment of various cyber security frameworks/standards, Putrus has written numerous articles and white papers in professional journals, some of which have been translated into several languages. He has been quoted in publications, articles, and books, including those used in master of business administration programs in the United States. He can be reach at robertputrus@therobertsglobal.com.

Types of Risk a Third Party May Have on an Enterprise

When a third party stores, accesses, transmits or performs business activities for and with an enterprise, it represents a probable risk for the enterprise. The degree of risk and the material effect are highly correlated with sensitivity and transaction volume.

> **"When a third party stores, accesses, transmits or performs business activities for and with an enterprise, it represents a probable risk for the enterprise."**

Enterprises are ultimately responsible for safekeeping, guarding and complying with regulation and law requirements of the sensitive information regardless of the contract stipulation, compensation, liability or mitigation stated in the signed contract with the third party.

Outsourcing certain activities to a third party poses potential risk to the enterprise. Some of those risk factors could have adverse impacts in the form of, but not limited to, strategic, reputational, financial, legal or information security issues. Other adverse impacts include service disruption and regulatory noncompliance.

The process approach in this article parallels the 2017 US Office of the Comptroller of the Currency (OCC) examination procedures that supplement OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance."[3] The supplement outlines key processes to manage the risk of third-party relationships. Its processes could well be extended as best practices for industries beyond financial enterprises. Its processes are:

1. **Life cycle phase 1: Planning**—Management develops plans to manage relationships with third parties.
2. **Life cycle phase 2: Due diligence and third-party selection**—The enterprise conducts due diligence on all potential third parties before selecting and entering into contracts or relationships.
3. **Life cycle phase 3: Contract negotiation**—Management reviews or has legal counsel review contracts before execution.
4. **Life cycle phase 4: Ongoing monitoring**—Management periodically reviews third-party relationships.
5. **Life cycle phase 5: Termination and contingency planning**—Management has adequate contingency plans that address steps to be taken in the event of contract default or termination.

Oversight and Approach to Third-Party Data Security: The Development of the Risk Register

It is the intent of this article to introduce a credible, objective and supportive measurement illustrating the degree of compliance and oversight demanded from third parties in proportion to the degree of risk to which the enterprise is exposed.

Data security extends to the third-party relationships in the areas of, but not limited to,

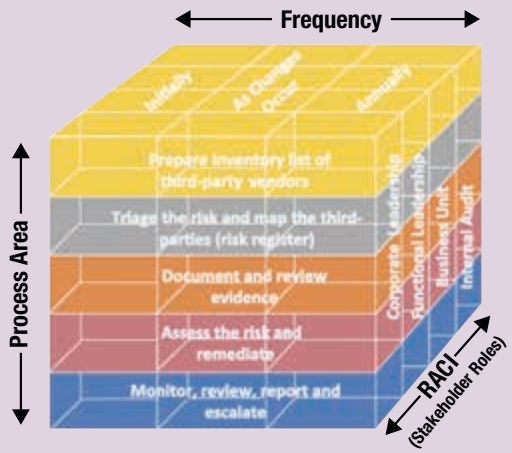
outsourcing IT services, applications, systems, infrastructure and transaction processing. The impact of third-party data security encompasses the enterprise's operations, supply chain, information technology and security, all levels of management (including the board of directors), and much more. Due to the impact that data security has on the enterprise, the representation of the stakeholders from different parts of the enterprise in the due diligence assessment and decision making is well justified and is left to the discretion of management as they deem appropriate.

The proposed systematic approach assumes that stakeholders are contributors to the efforts, reports, conclusion, recommendations and decisions related to third-party data security risk and compliance.

The foundation of the proposed assessment methodology is broken into three dimensions, as illustrated in **figure 1**:

1. **Process area**—This represents the degree of risk and compliance against which third parties are measured. It represents the development steps of the risk register, which is the critical and final outcome of the methodology presented in this article. The development and conclusion of the risk register is a successive approach represented by five tiers.
2. **Frequency**—This is the repeatable period or schedule of the examination/reporting required from the third parties by the enterprise receiving the services. The frequency is an integral part of the risk register since it relies on the third-party levels of risk and types of substantiated required evidence.
3. **Responsible, accountable, consulted, informed (RACI)**—This is the roles and responsibilities model for any activity that the stakeholders of the enterprise manage and oversee. The RACI cross-functional stakeholders could be drawn from various departments such as compliance, information technology, supply chain, legal and human resources. The basic elements of the RACI model are:
   - **Responsible**—The stakeholders who perform the work
   - **Accountable**—The stakeholders who are accountable for the work and decision making
   - **Consulted**—The stakeholders who must be consulted before decisions are made and/or tasks are concluded
   - **Informed**—The stakeholders who must be informed when a decision is made or work is completed

Figure 1—Risk-Based Model of Third-Party Data Security and Compliance



The Proposed Process Approach

The following are the recommended procedural steps of the risk-based management approach:

- **Prepare inventory list of third-party vendors**—One size does not fit all. When compiling the list of third parties and developing the criteria to assess the third parties' security risk to the enterprise, the list must be within the context of the industry, types of rendered services and the degree of impact of service dependencies on the enterprise. The enterprise's expectations of third-party data security compliance will vary and depend on:
  - The business relationship and what is rendered (products or services) by the third party—e.g., if the nature of the rendered services is transactional data, the Statements on Standards for Attestation Engagements (SSAE) 18 is effective for Service Organization Control (SOC) report opinions.
  - The criticality to the core processes of what is rendered to the enterprise—e.g., when the relationship between the enterprise and the third party is governed through information technology outsourcing (ITO) services.

Enjoying this article?

- Read *Vendor Management Using COBIT® 5.* *www.isaca.org/vendor-management*

– The data and cyber security impact that the third party has when there is a data exchange/transmission with the enterprise—e.g., what are the methods of secure transmission and types of encryption used to transfer data, such as confidential or proprietary information, over a secure channel?
– The type and nature of the data exchange (intellectual, product, financial, human resource, health, private) between the enterprise and the third party—e.g., the compliance of data exchange related to the patient health information is governed in the United States under the Health Insurance Portability and Accountability Act (HIPAA).

"Depending on the services rendered, the third party may exert multiple risk factors on the enterprise, which will increase the due diligence and compliance assurance required from the third party."

– The entity type of the third party (e.g., public, private, government)—e.g., if the entity is a US government agency, it will require compliance with the US Federal Information Security Management Act (FISMA). This act requires each federal agency to develop, document and implement an agencywide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source.

- **Triage the risk and map the third parties (risk register)**—When dealing with a third party, the enterprise must examine the types of risk that are posed. Depending on the services rendered, the third party may exert multiple risk factors on the enterprise, which will increase the due diligence and compliance assurance required from the third party.

The risk level must be assessed and recorded in the third-party risk register as critical risk, moderate risk or low risk. This is mostly a qualitative assessment, determined by the RACI team and guided by the risk categories, which include:

– **Strategic risk**—This is dependent on the uniqueness and the volume of the transactions that are offered by the third party. This is the risk that happens when the value to the enterprise is highly aligned with technology risk management. For example, large enterprises may rely heavily on a third party for technology support and processing critical information. Safeguarding informational assets will impact the enterprise's value and reputation.
– **Information management and security risk**—This is a combination of information technology services, information technology security and regulatory compliance risk. For example, a from-and-to transfer of information will pose a number of security challenges, such as data security during the transmission. Additional risk factors include confidentiality, user access, media location, physical security, device security and fourth-party risk, if any.
– **Resiliency risk**—This is related to the enterprise's mission-critical activities and how resilient the third party is to ensure information availability, disaster recovery, business continuity, incident management, recovery time objective (RTO), recovery point objective (RPO) and single point of failure (SPOF).

There could be regulatory compliance expectations or key controls in place that are exclusive to the third-party industry type, nature of rendered services or market capitalization. For example, the third party may require complying with the US Sarbanes-Oxley (SOX) Act, HIPAA, the US Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard

(PCI DSS), and the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)'s ISO/IEC 27001 or presenting attestation reports such as SOC 1 or SOC 2. These requirements must be taken into consideration when assessing the risk categorization of the third party. However, in the absence of regulatory compliance attestation reports, the enterprise must treat the third party differently. The enterprise may require an on-site assessment or send a questionnaire to be completed by the third party at a frequency that the enterprise deems appropriate.

In addition, the enterprise may establish red-flag rules when there are internal or external events taking place that impact the third party and the control environment and that impose significant risk. Some of these events could be merger and acquisition, divestiture, major organization changes, entering new markets, and geographic expansion. Such events will justify the enterprise to demand assurance in the form of a new security assessment or evidence that the key controls are in place and operating effectively.

- **Document and review evidence**—The enterprise will determine the appropriate documents required of the third party to produce and present. This is based on the entity's type and the nature of the business relationship.

For publicly traded companies, an enterprise located in the United States may request and examine reports related to SOX compliance, HIPAA, GLBA, PCI DDS, SOC 1, SOC 2 or ISO 27001. That may be sufficient as evidence that the third party has the key controls in place, and this must be asserted by the senior executives.

In Canada, there are broad laws that regulate security and privacy, such as the federal Personal Information Protection and Electronic Documents Act (PIPED) Act; Bill 198, referred to as Canadian SOX (C-SOX); the Health Information Protection Act; and regulatory standards set by PCI DSS.

In Mexico, there is the Law on the Protection of Personal Data Held by Private Parties. In Europe, there is the European Union Data Protection Directive. In Japan, there is a statute that covers internal controls for public companies. It is referred to as J-SOX.

However, the other category of third party, i.e., a third party that has no regularity compliance reports to provide, may require the enterprise to perform an audit, a walk-through or complete questionnaires as the needed evidence that key internal controls are in place and operating effectively. The frequency (six months, annual or biannual) of the data security assessment will depend on the risk category that the enterprise has determined. It is critical to have the types of reports and the frequency of examinations of the key controls stated when the contract is negotiated or renewed.

The type and frequency of data-security-related evidence or documentation for the third party to substantiate must be logged in the third-party risk register that the enterprise maintains.

"It is critical to have the types of reports and the frequency of examinations of the key controls stated when the contract is negotiated or renewed."

- **Assess and remediate the risk**—The objective of this step is to complete the development of the third-party risk register with a built-in scoring technique to assess and aggregate the risk for each individual third party. This register should use the risk category levels of critical risk, moderate risk or low risk, as described earlier.

The individual third parties will be classified and placed in the appropriate risk category with the approval of the enterprise RACI team. In the third-party risk register, the enterprise will specify the required document to be produced by the third party, the frequency and any remediation or additional controls that may mitigate the risk to an acceptable level.

- **Monitor, review, report and escalate**—Monitoring, reviewing and reporting third-party risk is an ongoing process. It should be performed on a regular basis and also be triggered if certain events take place, such as merger and acquisition, divestiture, major organization changes, entering new markets, and geographic expansion. The third-party risk register will provide guidance for the enterprise's required action and follow-up.

  The RACI team represents the appropriate balance of the required governance for the enterprise's follow-up, escalation, accountability and decision making. This provides authenticity, legitimacy, objectivity, credibility and support to the third-party risk process.

Walk-Through Example

The following is a hypothetical example that is used to determine the constituted risk and to develop a third-party risk register using the approach proposed in this article and the following assumptions:

- Determining security risk measurement is the objective of the hypothetical example used. If the third party is unable to provide the regulatory compliance reports, it is recommended to use revised types of standards and/or an assessment questionnaire, such as the one presented in **figure 2**.
- Apply and roll out the process equally to all or selected third parties. As deemed appropriate, adopt the key controls from a published standard, such as US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, ISO 27001, the SANS 20 Critical Security Controls for Effective Cyber Defense, or develop a risk assessment. For the example illustrated in **figure 2**, the highest average score of risk (impact x presence) is 15. Risk is calculated based on the highest score of total risk (105) divided by 7, the number of assessment questions in **figure 2**.
- The number of third parties identified as being part of the evaluation is 80. This represents the number of entities that are sanctioned by the enterprise's RACI team to be regularly reviewed, evaluated, monitored and placed in the enterprise's third-party risk register.
- A scale of 1 to 5 is used to determine the impact and to amplify the significance of the stated controls seen fit. The scale is a subjective measure and is consistent with the definition of the risk categories and risk levels discussed earlier. The scale from 1 to 5 is determined and agreed to by the RACI team (**figure 2**).
- A scale of 0 to 3 is used to illustrate the presence of control, i.e., the degree of the operating effectiveness of the stated control at the third party (**figure 2**).
- An illustration of an aggregate risk for Third Party 1 is placed on the risk category scale. The aggregate risk of Third Party 1 is 7, which is the result of the calculation made in **figure 2**. It is left to the user of this methodology to determine the scaled range of critical risk, moderate risk and low risk (**figure 3**).
- All 80 identified third parties should be mapped according to **figure 2** and **figure 3**.
- The third-party risk register is used to classify where the third party is placed with respect to the risk categories and the expected documents to be produced and presented by the third party (**figure 4**).
- A summary of the total number of third parties and how many fall within the risk category (critical risk, moderate risk and low risk) is examined in **figure 5**.

Figure 2—Information Security Assessment Questionnaire: Key Controls

Information Security Assessment Questions	Impact (1–5)	Presence of Control 0=N/A,1= Yes, 2=Partially, 3=No	Risk (Impact x Presence) Subtotal
1. Governance of Information Security			8
1.1 Does the organization have written information security policies?	4	2	8
1.2 <list>			
2. General Security			4
2.1 Is antivirus software installed on every workstation?	4	1	4
2.2 <list>			
3. Network Security			5
3.1 Does the organization use demilitarized zone (DMZ) architecture for Internet systems?	5	1	5
3.2 <list>			
4. Systems Security			6
4.1 Does the organization implement encryption for confidential information?	3	2	6
4.2 <list>			
5. Resiliency: Business Continuity/Disaster Recovery			12
5.1 Does the organization implement redundancy or high availability for critical functions?	4	3	12
5.2 <list>			
6. Incident Response Plan			6
6.1 Does the organization have a written incident response plan?	2	3	6
6.2 <list>			
7. Auditing/Client Reporting			8
7.1 Will the organization provide relevant certificates of applicability, e.g., ISO 27001, SOC?	4	2	8
7.2 <list>			
TOTAL			49
Average Risk for Third Party 1 (Total/Total number of controls)=49/7			7.0

Figure 3—Aggregate Risk Category for Third Party

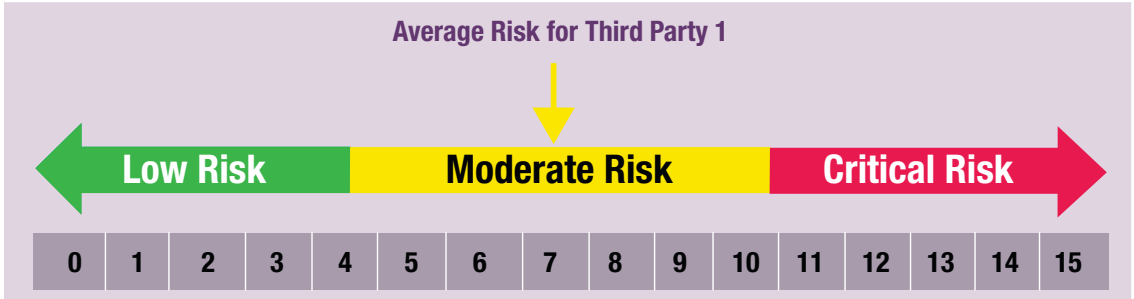


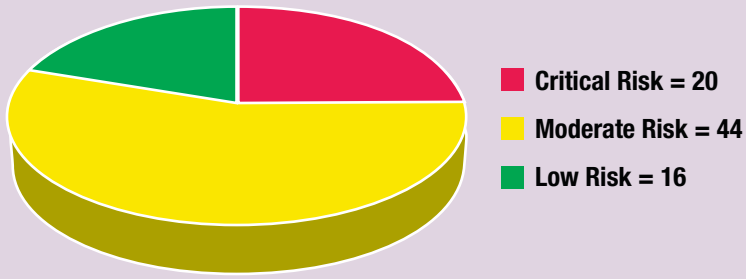
Figure 4—Third-Party Risk Register

Level of Risk	Control/Evidence Type	Frequency of Control	Internal Auditor	Business Unit	Functional Leaders	Corporate Leaders
Critical	SOC, PCI, HIPAA, SOX, external audit	Annual	R	A	C	I
Moderate	External/internal audit, self-assessment	Annual/as needed	R	A	C	I
Low	Self-assessment	As needed	R	A	C	I

RACI: R = Responsible A = Accountable C = Consulted I = Informed

Figure 5—Management Summary: Risk Examination of Third Parties

Total Number of Examined Third Parties	Third Parties Numbers of Risk Criteria	Third Parties Number of Risk Moderate	Third Parties Number of Risk Low
80	20	44	16



Advantages of the Outlined Process Approach

One of the challenges facing the enterprise in forming a team to manage third-party data security risk and compliance is the cost justification of such an investment. Using traditional accounting methods, such as discounted cash flow, to determine the return on investment (ROI) for cyber security initiatives may not be very suitable in this case.

A previous *ISACA® Journal* article, "A Nontraditional Approach to Justifying Cyber Security Investments," provides a platform for justification. It is based on the enterprise business model where objective, critical success factors (CSFs) and business challenges are all linked and supported by cyber security initiatives.[4]

Using a risk-based management approach to third-party data security risk and compliance can yield numerous benefits, including:

1. Establishing a single repository of third-party suppliers
2. Achieving the accountability and ownership needed to apply a consistent approach with all third parties and have expectations for supportive documents to substantiate risk management

3. Building trust by using the RACI model to ensure team cohesion on achieving desired outcomes. The credibility, accuracy and results of managing risk are highly dependent on more than one person participating in the areas of expertise that make up the RACI team and the cross-functional representations within the enterprise
4. Establishing risk-based segmentation of third parties based on categories established by identifying the third parties that are critical to the enterprise's well-being and identifying those that pose the highest risk
5. Developing and monitoring remediation and communication between the enterprise and third parties
6. Developing content for negotiating future contracts with other third parties
7. Providing timely communication and rapid response to changing regulatory requirements and third-party relationships
8. Improving compliance with federal, state, local and industry requirements
9. Streamlining efforts and maximizing staff productivity with a focus on high-priority third-party risk
10. Substantiating the enterprise's authenticity, objectivity and credibility by managing third-party risk

Conclusion

The trend of enterprises in various industries using third parties is on the rise. An Institute of Internal Auditors Research Foundation survey shows that 90 percent of respondents are using third-party technology. More than 65 percent of respondents rely in a significant manner on third parties.[5]

Consequentially, the risk exerted on enterprises parallels this trend. In the face of growing cyber security threats and compliance requirements, vast numbers of enterprises are seeking to determine the exposed risk and implement strategies to manage it.

This article presents a risk-based management approach to third-party data security risk and compliance through the development of a third-party risk register. It provides a systematic approach to evaluate and quantify the severity of and the exposure to risks presented by working with third-party vendors.

Once the level of risk is determined, the enterprise will be able to establish and dictate the type and frequency of support documents/reports required of third-party vendors so management can substantiate and assert compliance with laws, industry standards and best practices.

Endnotes

1 PricewaterhouseCoopers, *2013 Global State of Information Security Survey*, 2013
2 Soha Systems, *Third Party Access Is a Major Source of Data Breaches, Yet Not an IT Priority*, 2016, *http://go.soha.io/hubfs/Survey_Reports/Soha_SysteÙ_Third_Party_Advisory_Group_2016_IT_Survey_Report.pdf*
3 Office of the Comptroller of the Currency, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2013-29, USA, 30 October 2013
4 Putrus, R. S.; "A Nontraditional Approach to Prioritizing and Justifying Cyber Security Investments," *ISACA® Journal*, vol. 2, 2016, p. 46–53, *www.isaca.org/Journal/archives/Pages/default.aspx*
5 The Institute of Internal Auditors Research Foundation, *Closing the Gaps in Third-Party Risk Management Defining a Larger Role for Internal Audit*, 2013, *http://cdn.cfo.com/content/uploads/2013/12/Crow_IAA_Study.pdf*