Deloitte.

Outsourcing transparency evolution

How information transparency creates value across the extended enterprise

Outsourcing transparency evolution

Transparent communication is evolving for outsource service providers and their customers. Imagine a scenario where an airplane pilot didn't have a standard mechanism to communicate with air traffic control. The pilot is responsible for the safe operation of the aircraft, while air traffic control is responsible for maintaining the safe, orderly, and efficient flow of air traffic throughout the global air traffic control system. The two must work seamlessly to fulfill their respective responsibilities and ensure safe travel for airline passengers. Similarly, in any outsourcing relationship, each party will have a different lens on the requirements, depending on which side of the relationship they represent.

According to Deloitte's 2016 global survey on Third-Party Governance and Risk Management, 87 percent of respondents faced a disruptive incident involving third parties within the past two to three years, prompting an increased focus on procurement-related risks.[1]

Customers

Customers are driving compliance to their extended enterprise risk management (EERM) strategy.

As companies execute an increasing amount of business outside the organization, managing the multitude of risks associated with outsourcing better, faster, and more cost-effectively requires a well planned and executed EERM program. This is especially important in the face of changing regulations, increased cyber threats, resiliency concerns, and operational risk factors. Reducing disruptions while sustaining and enhancing outsourcing relationships requires assurance that internal controls are in place and regulatory requirements are met.

Providers

Outsource service providers are responding to multiple requests from multiple customers.

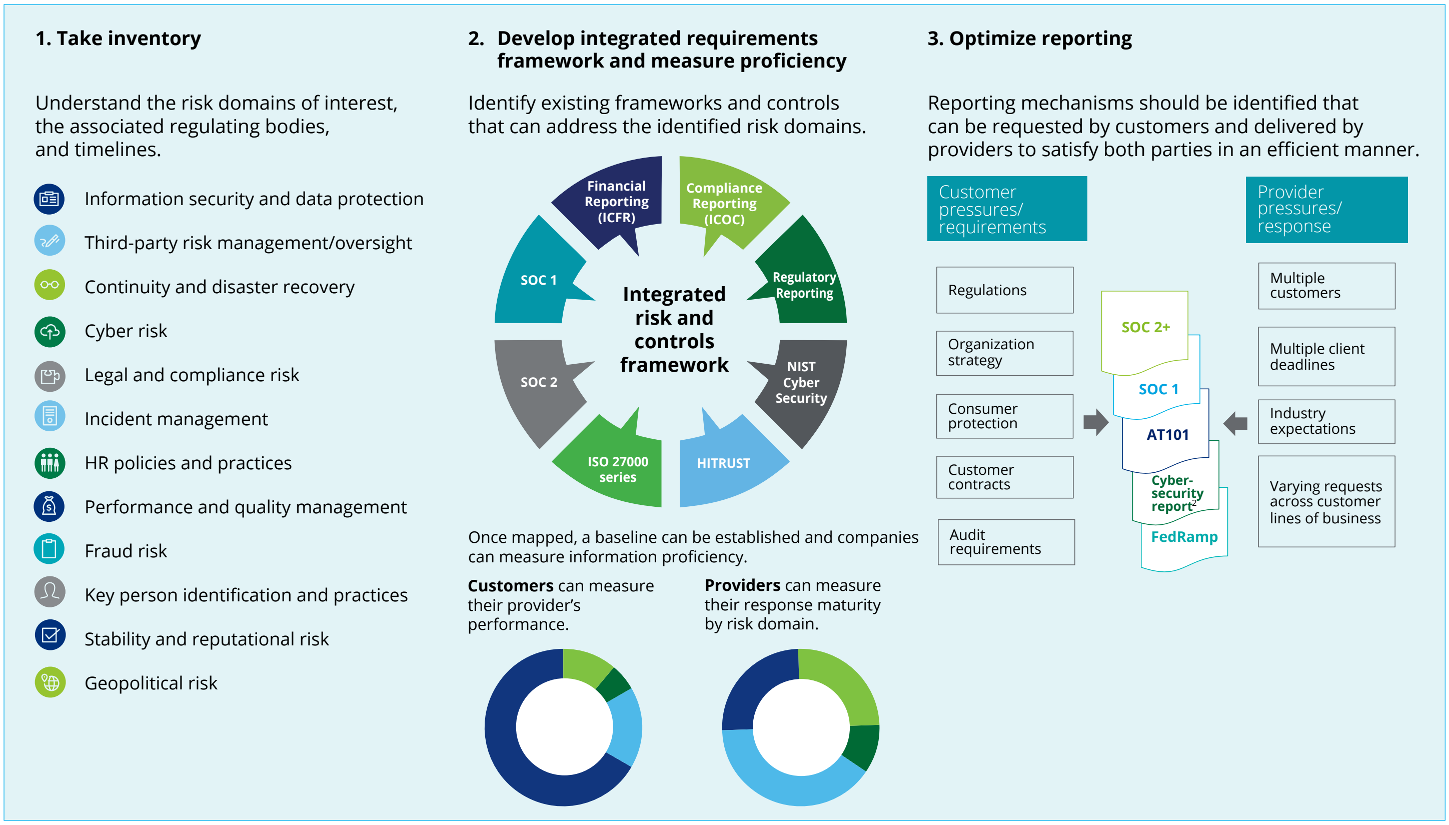
The depth and breadth of information being requested by customers is often inconsistent, unclear, and not always readily available. Increased reliance on technology, regulatory scrutiny, and cyber threats compels customers to quickly issue information requests so they can monitor their outsource service providers. Throughout a provider's customer base, and even across lines of business within a single customer, information is often requested repeatedly in multiple formats, adding layers of complexity and frustration to the process.

Open the dialogue

A key to a successful outsourcing relationship is "outsourcing transparency," which requires communication between the two parties on priorities and information requirements (Figure 1). For example, clear communication between an airline pilot (customer) and air traffic control (service provider) defines a set of responsibilities for each party and is critical to achieving safe air travel.

Because its mission is critical, the aviation industry has standard protocols and procedures for communication between its pilots and air traffic control. This is not the case in many other industries that haven't matured enough to establish a common understanding on what, when, and how information should be shared to achieve objectives.

Figure 1. How does the conversation evolve?



1. Take inventory

Understand the risk domains of interest, the associated regulating bodies, and timelines.

- Information security and data protection
- Third-party risk management/oversight
- Continuity and disaster recovery
- Cyber risk
- Legal and compliance risk
- Incident management
- HR policies and practices
- Performance and quality management
- Fraud risk
- Key person identification and practices
- Stability and reputational risk
- Geopolitical risk

2. Develop integrated requirements framework and measure proficiency

Identify existing frameworks and controls that can address the identified risk domains.

Integrated risk and controls framework
Financial Reporting (ICFR)
Compliance Reporting (ICOC)
Regulatory Reporting
NIST Cyber Security
HITRUST
ISO 27000 series
SOC 2
SOC 1

Once mapped, a baseline can be established and companies can measure information proficiency.

Customers can measure their provider's performance.

Providers can measure their response maturity by risk domain.

3. Optimize reporting

Reporting mechanisms should be identified that can be requested by customers and delivered by providers to satisfy both parties in an efficient manner.

Take inventory

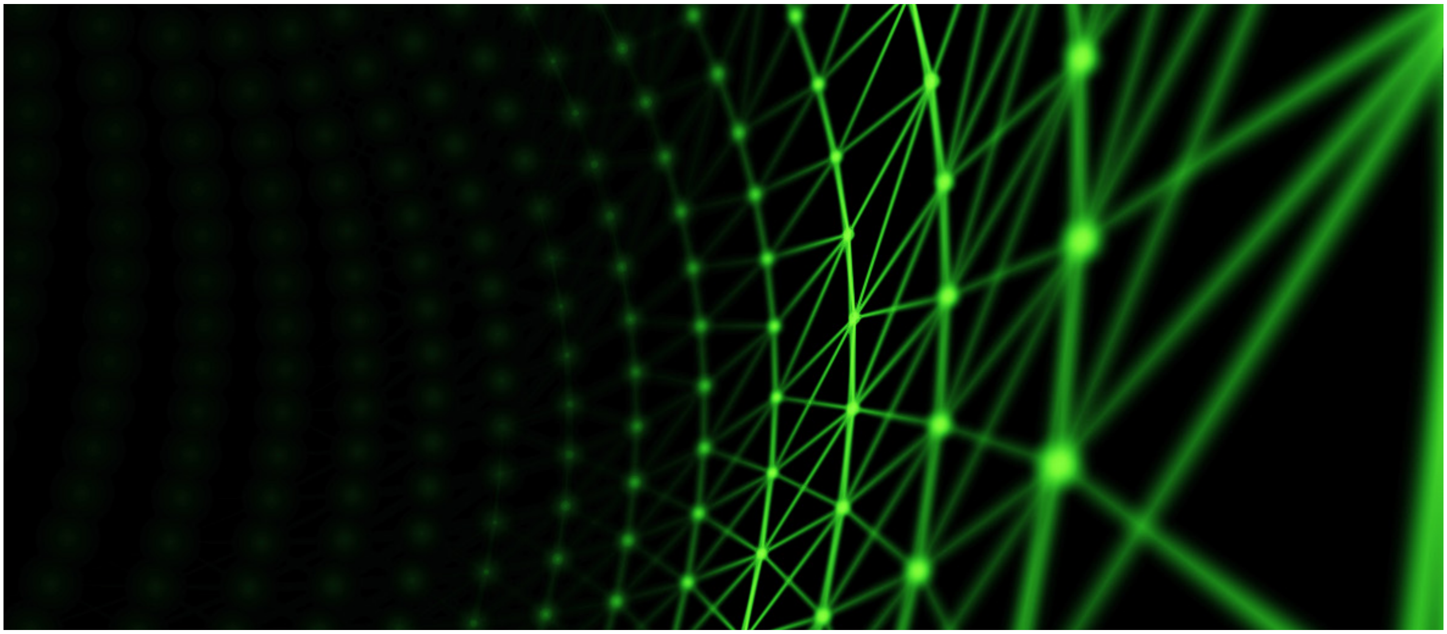
The marketplace will continue evolving to address the anxiety over outsourcing relationships. In the meantime, companies should take inventory, discuss requirements, and consider existing and future-state mechanisms.

Customers

Inventory risk domains and service provider relationships
By identifying risk domains and creating a matrix of providers that impact those domains, **companies** can risk weigh each provider. More critical functions may equate to higher risk, and require a higher level of information gathering and assurance requested of providers.

Providers

Develop mechanisms to proactively address customer needs
A proactive approach to understanding important milestones can enable **providers** to provide better information more efficiently. Reviewing existing customer contracts, holding focus groups, monitoring industry trends, and executing questionnaires to gather requirements helps companies develop a baseline for customer requirements.



Develop an integrated risk and controls framework

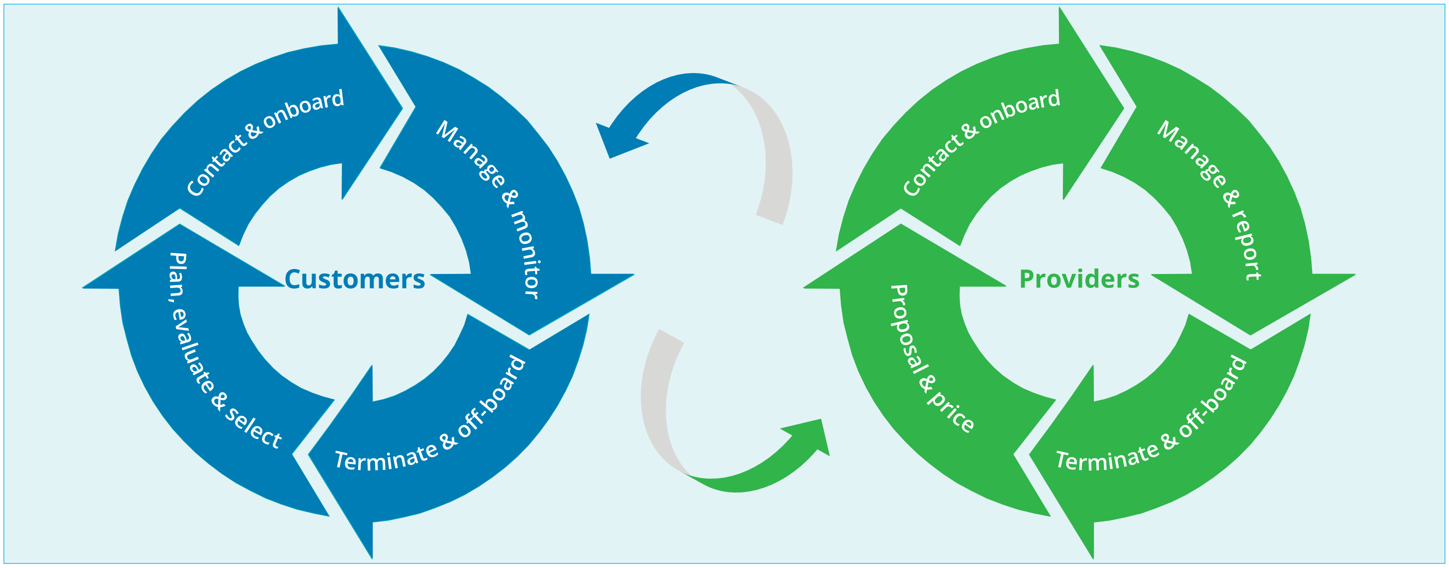
Determining what to provide, as well as when and how to supply it, plagues many service providers. Likewise, customers struggle with matching the level of risk to the information requested. Both sides can better define optimal transparency by:

Customers

Gathering regulatory and other requirements across lines of business and establishing a governance framework, which includes each inventoried risk domain, respective risks, and controls to ensure providers adhere to requirements. These requirements should be built into the provider cycle to establish guidelines on information flow for each phase. This can include the contract terms, service-level agreements, and information that will be shared to provide comprehensive oversight.

Providers

Streamlining and structuring reporting requirements into an integrated risk and controls framework to be more efficient and meet the needs of their customers with a consistent message across the company and throughout each phase of the outsourcing lifecycle.



Measure proficiency

Companies that reduce the cost and increase the efficiency of information flow can diminish the reality or perception of risk. Customers can eliminate providers that don't measure up to reduce risk, while providers that are transparent may offer opportunities for customers to involve them at a more strategic level where they can drive higher value. Learning how to use outsourcing transparency to manage risk and leverage provider capabilities can enhance competitive advantage for both sides. For most companies, effective third-party risk management can drive an additional four to five percent return on equity.[3]

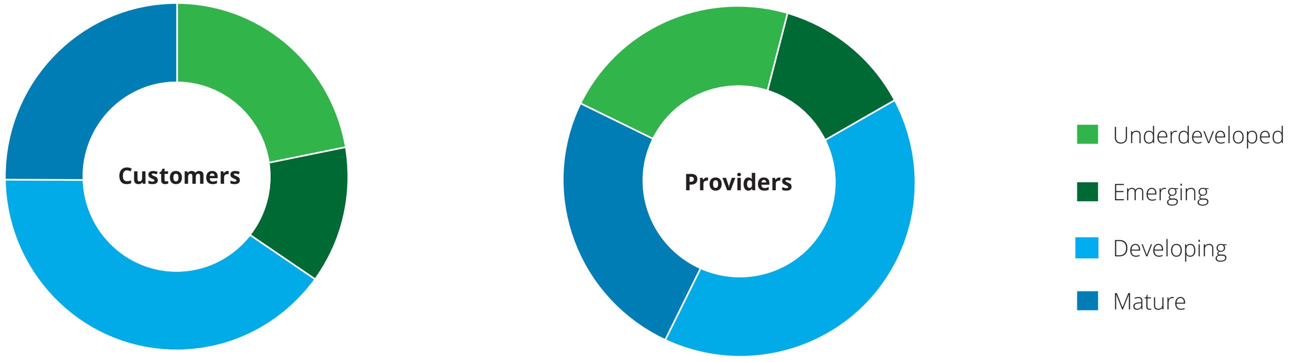
Companies need to define a baseline of acceptable risk tolerance for outsourcing transparency. This baseline can be established once the integrated risk and controls framework has been established, which will highlight gaps in control assurance. Measuring risk domains for maturity is becoming increasingly important as more stringent regulations drive the need for greater assurance through control frameworks, and therefore greater maturity in provider environments.

Customers

Customers can measure providers on their effectiveness at receiving, responding to, and delivering on information requests. Once a customer determines how providers rank against the baseline, they can take action to close gaps and reduce unnecessary overhead. This measurement technique can be used to make strategic decisions by ranking the quality of providers.

Providers

Using the integrated risk and controls requirements baseline, **providers** can identify gaps in controls across the organization and inconsistencies in communication with customers. The ability to respond to information requests in a cost-efficient and consistent manner can be measured.



Optimize reporting

Customers

Instead of requesting multiple pieces of information in various formats, **customers** can ask for specific independent auditor reports or control frameworks to satisfy their collective requirements.

Providers

Rather than reacting each time an information request comes in from a customer, **providers** can demonstrate a mature control environment by providing an independent auditor report mapped to the specific needs of the customer.

A number of mechanisms can be used to capture information including due diligence questionnaires, independent audit reports, ad-hoc reporting, internal audit site visits, etc. However, because most customers expect a personalized response to information requests, many providers struggle to cost-effectively deliver accurate and reliable data that can stand up to regulatory scrutiny.

Growing reliance on outsourcing has many companies managing thousands of provider relationships at any given time. Without a standardized process for assimilating and submitting information, managing and responding to requests remains inefficient and costly. External reporting mechanisms, such as independent auditor reporting (i.e., SOC 1, SOC 2, cybersecurity risk management examination [proposed][4]), can be requested and provided to realize substantial efficiencies during outsourcing transparency.

Balance value protection with value creation to drive performance

The relationship between pilots and air traffic control is clear. And the mission of safety could not be accomplished without both parties. Establishing transparent communications drives tremendous value to passengers, ensuring safer, faster, and cheaper worldwide travel.

As companies continue striving to attain a mature level of outsourcing transparency, implementing the steps discussed can add value by reducing redundant activities, improving efficiency, increasing cost effectiveness, and ensuring appropriate governance. Both parties should have an open dialogue to define requirements and how to address them in the most cost-efficient and effective manner.

Stay tuned as Deloitte continues to provide insights into the outsourcing transparency evolution conversation.

Contact us

Dan Kinsella
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 402 997 7851
dkinsella@deloitte.com

Adam Berman
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 7267
aberman@deloitte.com

Scott Gauch
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 213 996 5792
sgauch@deloitte.com

Carolyn Axisa
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 2820
caxisa@deloitte.com

Tom Haberman
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 513 784 7170
thaberman@deloitte.com

Walter Hoogmoed
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 973 602 5840
whoogmoed@deloitte.com

Endnotes

1 Deloitte UK Global Survey 2016, Third-party governance and risk management: The threats are real. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-third-party-gov-risk-management-2016.pdf
2 American Institute of Certified Public Accountants (AICPA) Cybersecurity Initiative. http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/aicpacybersecurityinitiative.aspx
3 Deloitte Consulting LLP 2016 Global Outsourcing Survey. https://www2.deloitte.com/us/en/pages/operations/articles/global-outsourcing-survey.html
4 American Institute of Certified Public Accountants (AICPA) Cybersecurity Initiative. http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/aicpacybersecurityinitiative.aspx

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" and "Deloitte Risk and Financial Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.