A Game of Risk

Organisations need a comprehensive process to effectively identify, quantify and actively manage risk through the lifecycle of their relationships with multiple third-party suppliers

Eleanor Winn IS A DIRECTOR AT ISG

Managing third-party supplier relationships is becoming increasingly complicated, and with complexity comes inherent risk.

In the current COVID-19 environment, with work-from-home orders and government lockdowns causing dramatic shifts in how work gets done, dealing with third-party suppliers has never seemed more risky.

Twenty years ago, a global organisation was likely to sign an outsourcing 'megadeal' – often a billion dollars or more – for the provision of multiple services. The management of that relationship was done under a single contract, with a single overall point of contact and a single (albeit huge) invoice.

In 2020, however, an organisation is more likely to work with tens, hundreds or even thousands of suppliers of all sizes, offering niche services, or specialising in specific areas. The result is a complex and demanding environment to manage: multiple contracts, SLAs, invoicing requirements, compliance regulations and relationship structures. And, of course, an extremely complex risk profile.

As a result of this fractured landscape, organisations are facing increasing demands on their time and resources to manage the potential risk posed by having so many third-party suppliers to oversee. To compound the difficulty, working with niche suppliers may mean that the organisation's own team may lack the specialist experience needed to fully understand the risks involved – leaving more room for error.

At a time when regulated industry businesses are under higher than ever levels of scrutiny from regulators, it is critical that they take a strategic, systematic approach to managing all their third-party relationships to minimise risk.

As with most things, data is at the heart of this approach. If you understand the data behind the risk profile for each supplier, then you can adjust your focus proportionately for effective risk mitigation. Relying solely on human attention and judgment leads, inevitably, to human error. As humans, we focus on the biggest risk potential first – which we assume will come from the biggest supplier. That can mean that smaller suppliers fly under the radar. A lapsed security certificate goes unchecked, an invoicing error isn't spotted, a contract renews automatically, a small data breach is unnoticed.

The answer is to use a combination of automation and humans to create processes that do not let the small things slip, and to keep a high-level view of the health of all your suppliers, not just the ones that issue the biggest invoices.

The Business Need

Every organisation needs to make sure that third parties are compliant and operating within the scope of the contract. Many will have entire teams dedicated to the management process. It's inefficient, ineffective and prone to human error.

To have a clear view of risk, you need a complete view of all your third-party relationships. Not just a single snapshot of what's happening right now, but what those relationships look like over their entire lifecycle.

Before starting the due diligence on a new supplier, every business should undertake a risk analysis process on that supplier. That should include looking at the potential for risk in different areas of the relationship and deciding what the impact of that risk might be. Does the organisation have the right processes and controls in place to mitigate all of these risks?

> **Relying solely on human attention and judgment leads, inevitably, to human error.**

Organisations often deal with multiple contracts over the lifetime of a single third-party relationship. When assessing risk, it's best to look at managing the total relationship with the supplier, rather than focusing solely on individual contracts.

The next step is to look at the risks of your suppliers as a whole – in other words, your supplier ecosystem. How do they work together? What interdependencies exist? When you're dealing with multiple suppliers, you need a system that allows you to track third-party lifecycle stages at a glance. Many organisations will not realise how many suppliers they are working with, so this is useful way to keep track of everything in one place.

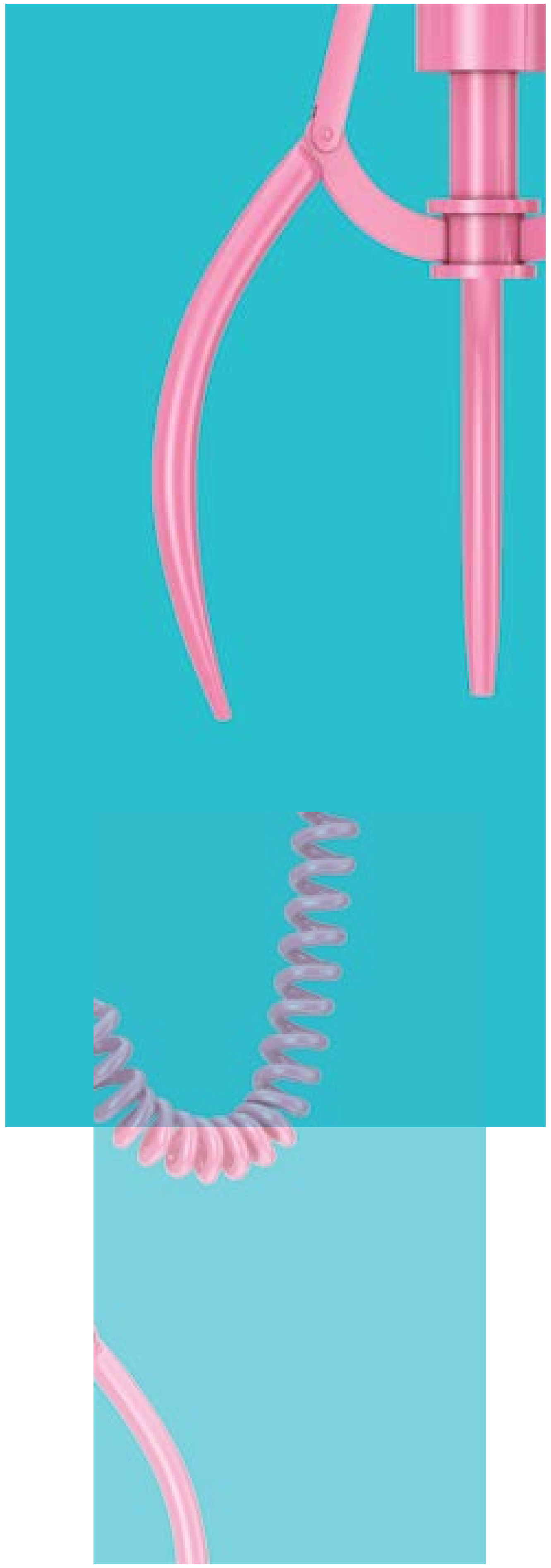
By looking at everything holistically, rather than just contract by contract, you can see, for example, when each contract comes up for renewal, which helps to mitigate the risk of overspend. I've worked with organisations where auto-renewed contracts have increased costs overnight by ten times – and no-one noticed in time to cancel or renegotiate the contract.

We recommend assessing risks by looking at seven areas:

Reputational risk. Assessing the impact to the organisation's reputation based on a failure or risk event caused by the service or products of the third-party.

Operational risk. Looking at the capability of the supplier to deliver the service. A good example here is the issue that struck KFC when a new supplier was unable to deliver chicken and other products to the fast-food chain's franchised restaurants. This should take into account not just the supplier, but all its subcontractors – fourth-party suppliers if you will – and the adequacy of the suppliers' technology and systems to manage its services.

Business continuity and resilience risk. This is absolutely front of mind for any organisation in light of COVID-19. Can the third-party still deliver in the light of a catastrophic event? This includes looking at their disaster recovery and business continuity plans and contingency strategies.



Information security and privacy risk. Assessing the third party's control standards that ensure the availability, confidentiality and integrity of information and data privacy, in line with current (and market-specific) regulation, and at what happens in the event of a data breach or security event.

Strategic risk. Assessing the macro trends that might affect the supplier, such as geopolitical, regulatory, legal and economic risk of sourcing to a country or region.

Regulatory risk. Assessing the third party's framework and ability to comply with regulations.

Financial risk. Assessing whether the supplier is financially stable and viable enough to continue to provide services or products. This includes ensuring the contracted terms allow the provider to operate in financial health.

Best Practice

There are several steps organisations can put in place to manage multiple third parties and mitigate risk.

Risk-tiering. Start by organising your third-party suppliers into tiers of risk. Doing this helps the organisation assign the resources needed to manage the risk that the third-party represents, and to deal with the potential impact of the problem. Different types of work will expose your organisation to different types of risks. For example, the business that supplies your printer ink and paper will pose a different level and type of risk to the one that manages your customer database. Risk-tiering also needs to be part of the overall risk assessment process.

Build risk management into all third-party contracts. Each contract should include clauses that clearly set out compliance and delivery requirements. Without these clauses acting as assessment criteria, it can be difficult to evaluate the ongoing risk that the provider represents. But, of course, whoever's managing the relationship has to know about those clauses to make them effective and have a process to track them.

Continually evaluate the work carried out by third-party suppliers. Collect and analyse data on work carried out by third-party suppliers to ensure their work remains compliant. The evaluation must be an ongoing process, especially for high-risk third and fourth-party suppliers. For example, if a new supplier tells you that they are ISO 2001 compliant, you need a system in place that requests and stores the certificate, knows when it expires and automatically asks for the new certificate. It's too important to simply accept the supplier's assurances without proof stored on your system. This is a process that can be automated to avoid human error or slippage.

Be vigilant. Watch for changes with the third-party supplier, or events that could lead to changes. Organisations need to stay on top of changes in their supplier's financial viability and ability to conduct the contracted work in a compliant manner. For example, one of your third-party suppliers may default on their financial obligations or find themselves in the middle of a reputational crisis. Factors like these could expose your organisation to higher levels of risk than usual, and so they need to be considered during the initial risk assessment, and the supplier continually monitored for changes to their circumstances.

> **Start by organising your third-party suppliers into tiers of risk.**

Take a global view. Monitor the macroeconomic and geopolitical environment your suppliers operate in – particularly if you've noted that there is risk potential as part of the initial assessment. For example, if the government of the nation that the supplier is resident in passes a law that negatively affects the supplier's business, it may have an impact on how well they can service your organisation. Note any significant people-related changes at the business, too, as these factors also involve risk to the ability to deliver against the contracted terms.

Whenever organisations commit to working with a third party, they are choosing to introduce an additional risk factor into the business. It's becoming more common for organisations to work with smaller, specialist suppliers, and therefore cultivate vast cohorts of suppliers that can be unwieldy to manage manually.

Organisations need a clearly defined process to manage third-party relationships throughout their entire lifecycle, to track compliance obligations and to make it easy to manage the various risks associated with working with the supplier. It's through this efficient and accurate management of supplier relationships that organisations can successfully mitigate third-party risk.