CONNECTED BUSINESS

…more need for Controlling the Chain of business activities

3RD PARTY RISK MANAGEMENT

OVERVIEW

1. The connected world is increasing

In the current business world companies are faced with increasing business dynamics. This demands for flexible organizations that can respond promptly in order to achieve its strategic objectives. Though in previous times companies tended to keep most of the required business activities within the own organization, newer business models are based on a hybrid of own and outsourced activities. In earlier days this was driven by more cost-effective motives and a great deal of production, helpdesk and software development activities were outsourced to countries with cheaper labor resources like China and India. More recently, the further evolution of digitalization brought (fintech) companies with excellent and innovative propositions. But this digitization will also lead to companies becoming more digitally interconnected and thus more dependent on each other. Indeed, this will result in more **dependency risks**. Regulators have noticed this development and are imposing new regulations on (financial) companies for enhanced risk management efforts with respect to their outsourced activities.

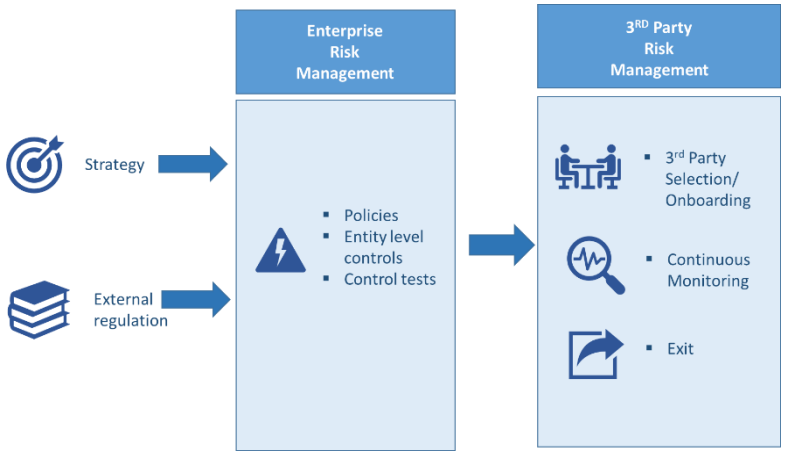
Examples of 3RD PARTIES

Companies operate in a universe with all kind of 3rd parties, for example :

- *Vendors that render services, deliver semi-finished products, raw materials or supplies;*
- *Outsourcing parties that take care of outsourced business processes, technologies or services;*
- *Customers;*
- *Asset managers that have mandates for managing a subset of financial assets;*
- *Business partners and channel partners (e.g. franchisers)*

2. Control Model for 3rd Parties

Despite the increased resilience that companies can create with co-sourcing and outsourcing of business activities, the dependency risks must be carefully managed. It is wise to apply a consistent control model which can be communicated and understand unambiguously by management and staff. In the chart below the context of such a control model is visualized.



The control model is split into two major pillars: one pillar relates to the overall risks for 3rd party risk management and is mainly triggered by strategic considerations and overall risk appetite, but also by external regulations. The other pillar relates the specific controls for mitigating risks associated with one single 3rd party.

- ***Strategy and Enterprise Risk Management for 3rd parties***

  *The ERM aspects of 3rd party risk management might differ per 3rd party category. The **vendor management strategies** (make-or-buy, distance or country preferences etc.) will be translated to vendor policies. From a risk point of view, potential overall vendor risks must be identified, risk appetite formulated and mitigating controls determined. Strategies may result is a high level of **outsourced activities**, but the company remains responsible and bear the risk for the resulting outcome of the outsourced activities. The reputation can be hurt significantly of the outsourcing causes business disruption, malfunctioning products, bad behavior etc. Likewise, vendors, the onboarding of new customers might cause risks if Know-Your-Customer policies have not been adapted properly in the organization.*

- ***External regulations and Enterprise Risk Management for 3rd parties***

  End services or products can be built up from a chain of business activities from multiple companies. Some products require traceability up to its raw materials origin (e.g. pharmaceuticals), others require companies that contribute to the value chain to comply with industry standards (e.g. ISO 13485 for medical devices). In the banking sector we see tightened regulations[1] for keeping control of outsourced business processes. And for Fintech companies (e.g. payment processing within the PSD2 regulation) it is important to comply with the requirements set by the interconnecting parties. It may be perceived as a burden in the first place, but ultimately strong control measures will raise the quality of the way of working. The ERM process at corporate level must be aware of current and foreseen compliancy demands and translate these into entity level controls.

[1] EBA guidelines on outsourcing arrangements, 25 February 2019, EBA/GL/2019/02.

The ERM pillar of the control model will result in a risk control life cycle within the 3rd party risk management pillar. Each 3rd party has a certain life cycle. The risk control process for 3rd parties can be split into three phases: the onboarding process, monitoring and adjustments during the life cycle and finally the exit process. In these three stages different aspects of risk mitigating measures are relevant.

- ***3rd party Selection and onboarding***

  The corporate policies and procedures will set guidelines for 3rd party selection. For example, at general level, certain industries or countries may be avoided due to corporate policy (e.g. exclude asset managers who are highly active in investing in carbon-intensive industries). Other policies may set standards for the selection process (e.g. minimum consultation of 3 parties). After selection, the preferred candidate must follow a risk assessment/ due diligence which may cover a wide variety of checks and assurance reviews. A check on qualifications for industry standards may be part of it.

- ***Continuous monitoring***

  If a 3rd party is accepted for onboarding this is not guarantee for an ever well performing relationship. Frequent monitoring is therefore needed and may involve operational due diligences that verify whether the assumed conditions (financial, operational, integrity, quality, compliance, service levels etc.) still prevail. This asks for a balanced monitoring process. For the outsourced activities, one cannot claim a driver seat in the management, but a tight control is needed. Assurance reports like ISEA3402 are often reported several months after the reported period itself (annually or semi-annually). This is far too late and not a right control instrument anymore in the dynamics of these days. Parties that are closely related in business activities should have a more digitally intertwined control mechanism. A combined framework with the status of the risk controls measures and metrics indicating the compliance with service levels could ideally be shared with digital communication.

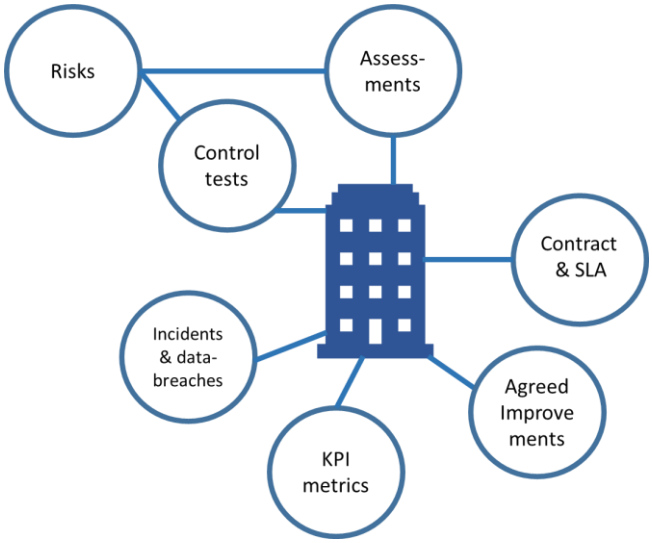
- ***Exit***

  Breaking up business relationships is not always easy. But transferring the outsourced business processes to other parties or even insource them again require a solid vigilance. Assuming the contract has a decent exit-clause, the execution of agreed exit activities (delivery of data and documents, transfer of knowledge, destruction of data etc.) requires adequate risk monitoring. The exit plan should be ready beforehand.

"DIGITALIZATION WILL INCREASE MUTUAL DEPENDENCIES OF PARTIES"

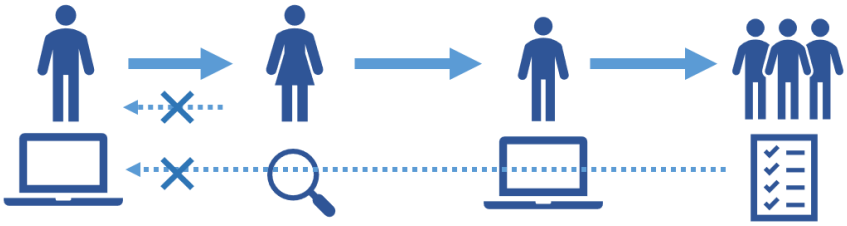
3. Technology enabled 3rd party management

CERRIX has embraced the previously described 3rd party control framework in their functionalities of the software. It contains a software module in which 3rd parties can be registered and monitored. The registration of a 3rd party contains all necessary data relevant for managing it. Documents like signed contracts and service level agreements can be attached to it with reference to the date of contract expiry. Predefined controls can be linked easily to the 3rd party. This can be a generic 3rd party control derived from the ERM control framework or a specific one designed for the specific 3rd party or the group it belongs to. If these controls are subject to frequent control tests and they fail, it might result in specific actions to be taken (e.g. Brexit legislation require to amend all UK contracts).



Today, it is quite common to send Excel spreadsheets via mail to execute an assessment for onboarding. With CERRIX, this process will become more efficient and also provide the necessary audit trails. The onboarding process for a 3rd party can be facilitated in CERRIX with predefined assessments forms. A form in CERRIX can be designed by a forms administrator. It consists of one or more webpages on which you can define text in any format, questions, requests for uploading documents, risk assessment widgets and many more. The number of pages is practically unlimited and the page-structure is part of your design preferences. The form can be sent to the potential new 3rd party. They will get access to the CERRIX form via a hyperlink in the mail and can immediately execute the assessment. After completion of the assessment, a notification mail is sent to the initiator who can then review the answers and accept or reject it (in that case sent back).

Optionally, the form can be built in such a way that it also includes a workflow that supports the internal assessment of the 3rd party acceptance process. For instance, the form is assessed by different departments (e.g. purchasing, legal, finance). Each workflow step can be set back to previous forms user in case the results are not satisfactory. Finally, the form results are stored into a forms register containing all assessment records and documents and can be retrieved at any moment in your preferred format.

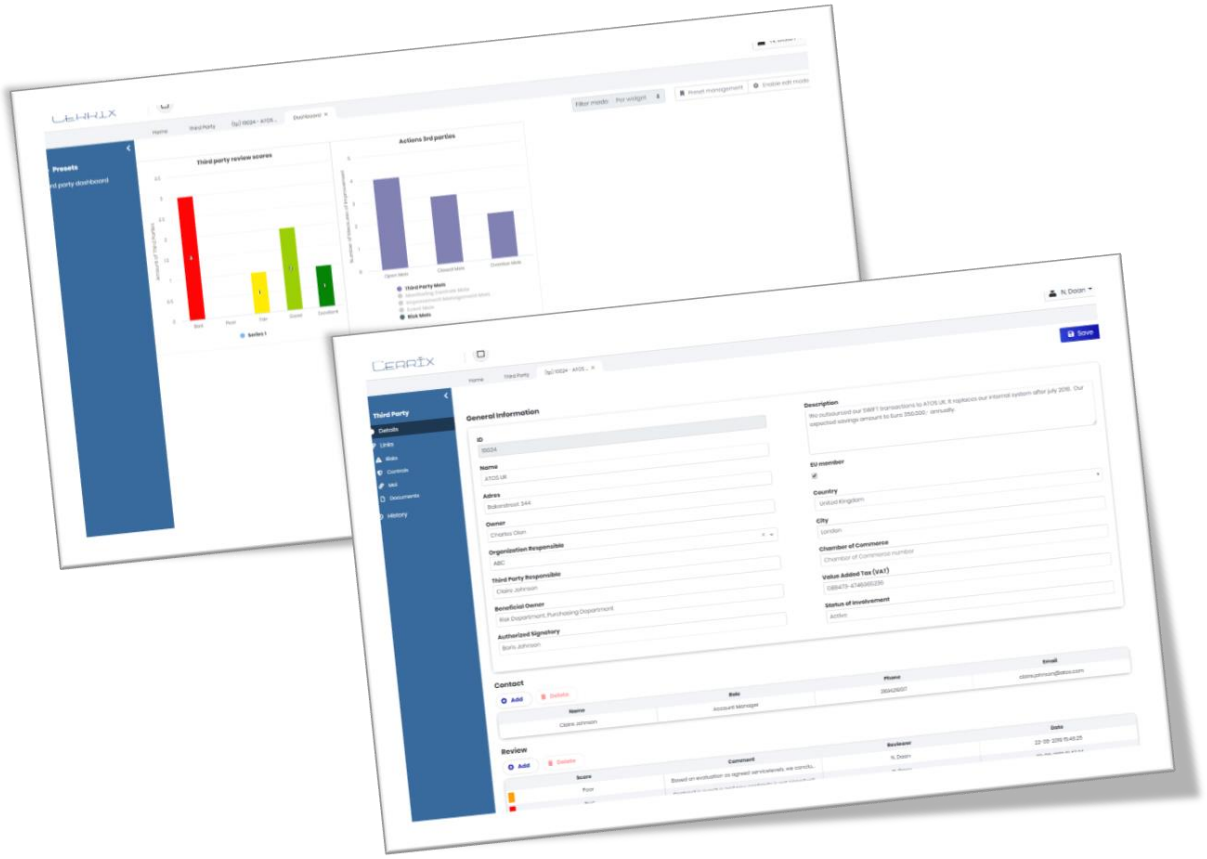


During the contractual phase with the 3rd Party, it is key to have an effective monitoring process in place. Internal monitoring is needed because many departments may make use of the services or goods of the 3rd Party. It is recommended to investigate the perceived satisfaction among internal stakeholders that have a relationship with the 3rd party. For this an assessment form in CERRIX can be used. If you want to re-assess the 3rd party this can either done with a form that can be sent to the 3rd Party but it can also involve an online review on market signals about this 3rd party (web crawlers can use Artificial Intelligence mechanism and scan market data, news and social media about a certain company). It can be vital for a company to know quickly if a client or vendor might become a risk for the company due to reputation, financial distress etc.

Serious incidents that occur at the 3rd party must be reported instantly to the company. It may happen for instance, that the company is responsible for privacy assurance of customer data that is outsourced to a 3rd party data processor. CERRIX offers the possibility to have a real-time digital connection with the 3rd party, who can register the incident in CERRIX and will automatically alarm the right stakeholders within the company.

The periodic 3rd party (internal and external) assessment might result in business improvements for the 3rd party. In CERRIX, these improvements can be assigned to the 3rd party automatic triggers will inform whether the due date is passed, or the action is completed.

A continuous monitoring also may include to measure certain metrics on a frequent basis. A common practice is the monitoring of agreed service levels. Rather than preparing 100 pages of service level reports, it is much more efficient for both parties if the 3rd party can deliver the datapoints digitally (e.g. Application Programming Interface, shortly API). In CERRIX, the tolerance levels can be set beforehand so that any breach of the threshold will give automatic notifications.



Many reasons might end the relationship with the 3rd party. Generally, legal contracts contain a clause describing the exit procedure and stipulate the obligations for both parties enabling a smooth exit process. Nevertheless, in the exit process, one must be cautious since the economic value of the contract for the 3rd party has disappeared and may increase operational risks. Data quality and timely transfer of data, business activities and governance require good project management.

SUMMARY

- 3rd Parties are subject to frequent reviews;
- Reviews can be based on internally and externally executed Assessments;
- In the CERRIX dashboard, a 3rd party widget can be used indicating the latest status of reviews for all (filtered) 3rd parties;
- Assessors and 3rd Party owners are triggered automatically for contract expiration, monitoring and action follow-up;
- Digital interconnection with 3rd parties for shared risk control can be established.

CONTACT US

Are you interested in more information about CERRIX solutions?

CERRIX
Koninginnegracht 29
2514 AB THE HAGUE
THE NETHERLANDS
☏ +31 (0) 70 363 77 33
info@CERRIX.COM