Using Automation to Build a Consolidated View of **Third-Party Risk**

Camms.
Software to change tomorrow.

Intro

Every organisation relies on a network of third parties to keep their operations running smoothly. Even the smallest organisation can have dozens of relationships that they depend on for goods, services, and technology - and larger businesses can expand into the hundreds or even thousands.

Keeping track of a complex network of vendors and third parties can be a challenge for risk & procurement teams - leaving many suppliers being individually managed by the teams that directly use their products and services. But without a central point of oversight, and a consistent way of rating and monitoring vendors, many organisations leave themselves vulnerable to unforeseen risk.

Your third parties are an extension of your business, you may have a great product, but if your website was down or the courier who delivered it was slow, the customer will have a negative experience with your brand.

But how reliable are the vendors and suppliers that you depend on? The failure of one key vendor can often be enough to stop an organisation in its tracks. How can organisations get a holistic view of vendor risk and put steps in place to ensure they are using a network of the most reliable vendors that won't cause unnecessary risk.

In This eBook We Explore:

- What an effective third-party risk management programme looks like.
- The problems with manual vendor risk management processes using spreadsheets.
- Tools & techniques to automate the vendor risk process.
- How to get a consolidated view of third-party risk across your organisation.
- How to get vendor risk on the boardroom agenda.
- How to bring vendor risk assessments & questionnaires online.

What is Third-Party Risk

Third-party risk management refers to the process of identifying, assessing, and mitigating the risks associated with the use of external vendors, suppliers, or partners who provide goods, services, or support to an organisation. Third-party risk management involves evaluating the risks posed by these third-party relationships and implementing controls to manage and mitigate these risks.

The objective of third-party risk management is to ensure that an organisation's use of third-party services does not result in any negative impact on the company's operations, reputation, or compliance with regulatory requirements. A third-party risk management programme typically involves establishing a formal onboarding & offboarding process, building a register of all third party vendors and conducting due diligence via risk assessments, questionnaires, surveys and score carding, establishing & monitoring performance metrics, and implementing risk mitigation strategies to ensure that the third-party relationships are conducted in a secure and compliant manner.

Comprehensive third-party risk management programmes will establish a risk appetite - based on a series of Key Risk Indicators (KRIs) and SLAs - that vendors must adhere too, and controls are set to flag problems and address substandard performance. Effective third-party risk management helps organisations to minimise the likelihood and impact of third-party risks and to protect their assets, reputation, and customer relationships. It also helps them to compare vendors and select the best provider by understanding their impact on business performance. The reports & vendor profiles generated as part of the programme provide all the data needed to conduct thorough vendor performance reviews and to support with decision-making when selecting and changing vendors.

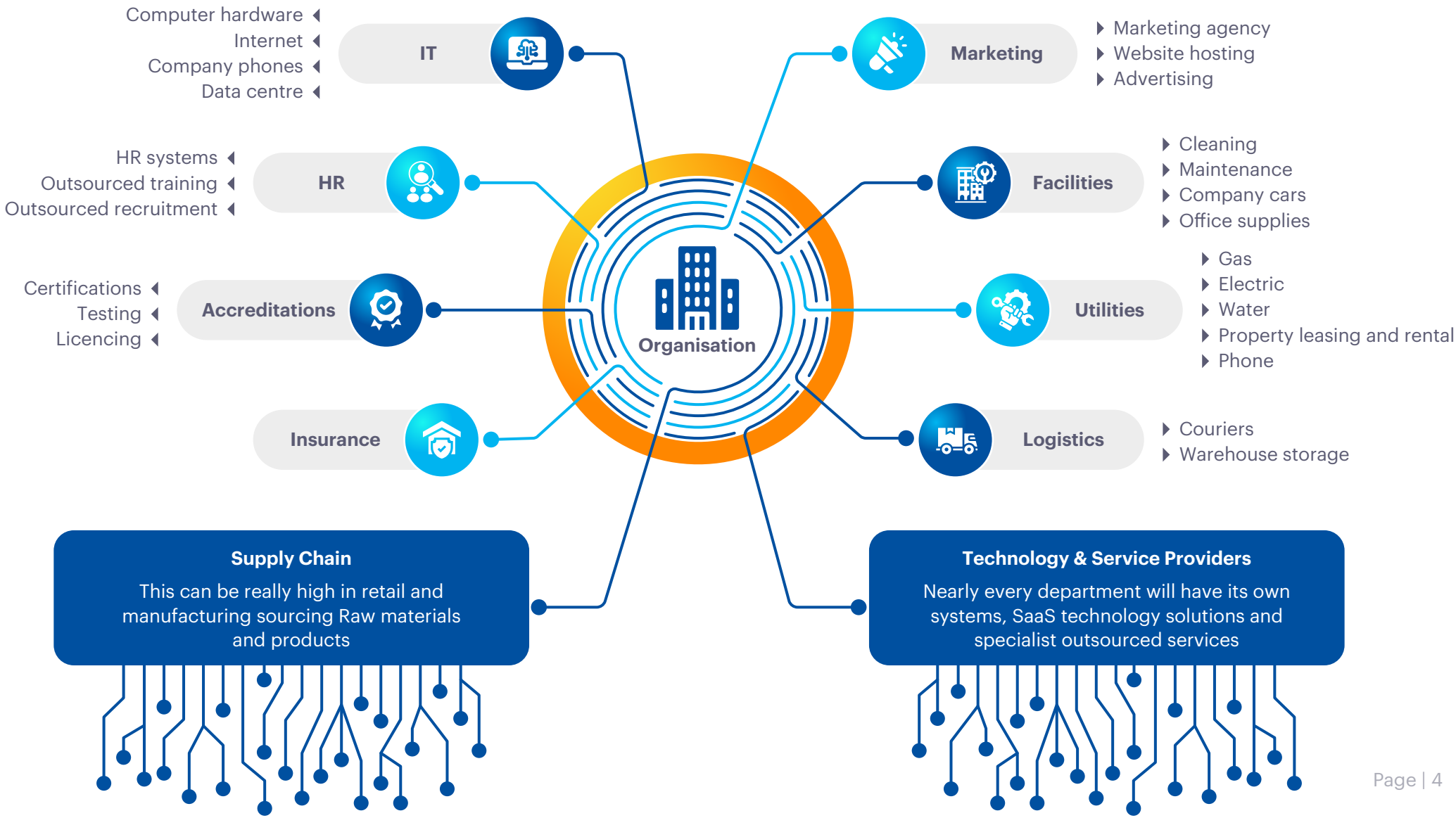
Today's modern businesses rely on a complex network of suppliers, technology providers, manufacturers, distributers, and service providers to run their organisations. The failure of one key third-party can have a catastrophic effect on the ability of an organisation to provide its goods and services.

Let's look at the typical network of third-party providers outsourced by an average mid-sized organisation. This can be much broader and even more interconnected for firms in retail and manufacturing who rely on suppliers and manufacturers for their raw materials and goods.

The Extended Enterprise

An organisation does not operate in isolation. It is supported by a complex network of third-party vendors. Here we map out a typical vendor network and this can increase exponentially for companies who have procurement and purchasing departments and buyers dealing with large supply chains to source raw materials and products.

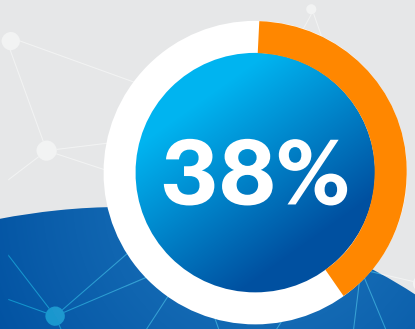
A Typical Vendor Network



Why is Third-Party Risk Management Important?

Third-party risk management is of critical importance to organisations. Your network of 'third parties' are an extension of your business. If your electricity or internet goes down or a vital supplier of raw material for your product goes bust - it can stop your business in its tracks. If you outsource work to manufacturers who provide substandard products or couriers that deliver late & damage parcels, your customers will have a bad experience leaving your reputation in tatters. Your choice of vendors directly affects how you perform as a business.

According to a KPMG survey



of organisations have experienced significant disruption, monetary loss or reputational damage as a result of a third party in the last 3 years.

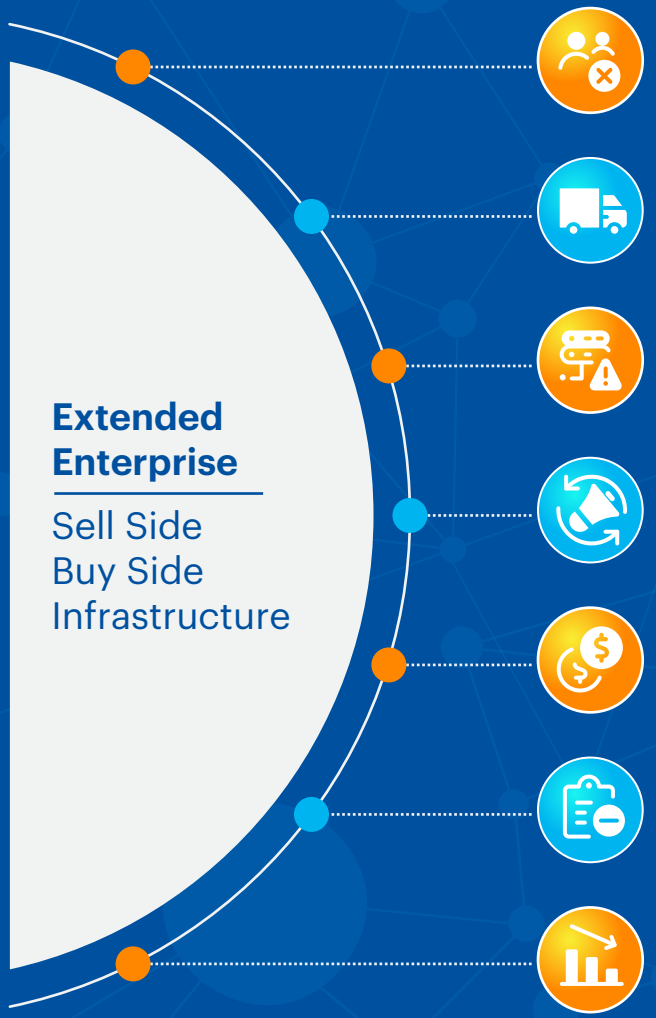
Reliable suppliers and service providers form part of your 'extended enterprise' and should ensure the smooth running of your organisation. That is why firms should implement strict on-boarding and procurement processes when selecting vendors - and monitor their work on an ongoing basis with regular risk assessments & scoring. Incidents and breaches of SLA's should be logged and monitored and worked through to resolution.

> The term third-party builds a stigma of something being a commodity, expendable, and changing. The strongest third-party risk (GRC) management programmes are focused on the extended enterprise and treat their third parties as critical players and partners to their strategy, operations, and processes.
>
> **Michael Rasmussen – GRC Pundit at GRC 20/20**

Without a centralised third-party risk management process, vendors and suppliers often end up being managed in silos by the departments that require and use their services. On a small scale this can work, but in mid to large organisations with multiple vendors this becomes problematic - as vendors become interlinked to a point where if one fails, other contracted vendors and service providers can't perform their function. Without a centralised third-party risk management programme organisations lack visibility of which vendors are the most critical, which are reliant on each other, and which ones are performing poorly or likely to fail. This lack of oversight deprives business leaders of vital information, making it difficult to allocate budget & resources and make contingency plans to ensure the smooth running of business operations continues.

Third-party risk management is even more important in public funded services, like schools, hospitals, and government - where taxpayers demand to know how their money is being spent, and there are huge risks of bribery and corruption with contracts being awarded unfairly.

Potential Third-Party Risk from an Extended Vendor Network



Loss of reputation - Risk to the reputation of the organisation from the use of third-party relationships can occur due to a myriad of reasons, including misuse of intellectual property, poor product quality, lack of compliance to human rights, and environmental regulations, etc.

Supply chain disruption - Key third-party business disruptions can occur due to bankruptcy, geopolitical issues, and macro risks can result in supply chain disruption.

Data risk - Loss, misuse, or mishandling of critical data of the organisation or its customers by a third-party relationship can result in financial loss, hefty fines, and decrease in shareholder value.

Product recall - Poor product quality, safety issues, or faulty packaging by third parties can lead to product recalls resulting in unforseen costs, lawsuits from consumers, increased costs from settlements, and lost revenue from missed sales opportunities.

Financial impact - Financial loss can result from under-reporting of revenue from licenses, royalty partners, distributors, franchisees, and over-payment for services from third-party relationships.

Lack of compliance - Third party acts corruptly to gain business advantage for the organisation resulting in hefty fines or the third-party is not in compliance with the relevant regulations followed by the organisation causing problems.

Poor performance - Lack of sustained performance from third-party relationships, can result in costly mistakes, over allocation of capital to oversee relationships, and defeating the purpose of outsourcing strategy.

Source: Deloitte Global Third-party Risk Management Survey 2022

Why Does Third-Party Risk Need to Be Managed Centrally

Over the last 20 years we have seen many organisations transform their operating models, taking advantage of the latest technology, products, and specialist solution providers to modernise and streamline their business processes.

Long-term partnerships form, and external parties become further integrated into the organisation and become an extension of the organisations operating model. But there is not an infinite budget and endless resources to continue with every vendor relationship forever, therefore it Is important to get a holistic view of all your third parties in one place to understand - who they are, how they are performing, how much they cost, what functions they support, how critical they are to the organisations infrastructure, and what are the associated risks of working with that supplier. Doing this in isolation for each third party does not enable organisations to see the bigger picture – making it impossible to make critical decisions on where budget, time, and resources should be increased or cut back.

Third-party risk management also needs to be managed centrally to easily compare vendors. Suppliers should be benchmarked against each other using your preferred scoring criteria - and rated based on industry standards - with regular assessments to ensure the organisation is using the most reliable yet cost effective network of vendors.

How Does Third-Party Risk Management Usually Start in Small Organisations?

Third-party risk management as a process doesn't tend to exist in small start-up organisations - usually various vendors and suppliers are managed by the individual teams using the products & services. For example, the accounts team look after the accounting software, IT staff look after any IT services, and buyers deal with supply chains.

In these less mature organisations selecting third parties will usually consist of getting a series of quotes and choosing a vendor based on a good feeling at an acceptable cost. Onboarding would usually be the signing of a contract from the vendor without any official checks. Any problems would be addressed with the supplier on an ad hoc basis as they arise. There would be little visibility around how the failure of that particular vendor could affect other business processes, and there would be limited contingency plans for the failure of the supplier. Often there would be little to no consideration of the suppliers cultural fit, for example - do they uphold the same values as your own company or follow the same compliance guidelines and standards? In less mature programmes there is often a lack of official benchmarking against other suppliers in that space or the performance of other vendors the organisation works with.

But as organisations grow and expand - and decisions must be made regarding where to allocate budget & resources or reduce costs - organisations realise they need a centralised view of their vendor network to balance the money, time, and resources allocated to each vendor. Organisations also need a holistic view of any potential risks resulting from each supplier relationship and to understand the performance of each third-party. As businesses expand so too does the interconnectedness of their third-party relationships and understanding the reliance certain business functions and other vendors have on each other becomes essential to understand the potential risks involved - and this requires extensive mapping.

Organisations who recognise the need to consolidate their third-party risk management into a centralised process should:

- Build a centralised register of their vendors.
- Establish a centralised rating framework to enable comparisons between suppliers based on their criticality, cost, and performance.
- Engage with owners of every supplier relationship across the organisation to gather essential details on each vendor.
- Establish KRI's, KPI's and SLAs for each vendor and decide which metrics will indicate if they are on track.
- Send out regular risk assessments and capture the results centrally.

Many businesses begin building out a third-party risk management solution using spreadsheets. They will often start by establishing a list of all vendors and their owners. From that point on they will send out a series of vendor risk assessments, questionnaires, and surveys via email to capture and log the critical information relating to each vendor. This information will be updated on an ad hoc basis as-and-when they roll out the next set of risk assessments, surveys, and questionnaires.

The spreadsheets are usually updated by hand when new vendor risk assessments, questionnaires, and survey results come in. Reporting is produced manually by creating one off reports for the board providing a moment in time snapshot of the data within the spreadsheet.

10 Signs You Need a Centralised Third-Party Risk Management Programme

1. You have no central view of all your third parties and their criticality.
2. You have no standardised onboarding and offboarding process.
3. Your network of vendors is managed in silos by the team who uses the service.
4. You are running vendor risk assessments on a manual ad hoc basis.
5. You struggle to get a centralised view of vendor performance and SLA's.
6. You lack proof that your suppliers & vendors are performing in line with the required policies, procedures, and compliance requirements.
7. You have insufficient controls to mitigate potential risks.
8. You have no standard way to score and assess vendors making comparisons difficult.
9. You lack third-party risk intelligence relating to vendor finances, sustainability ratings, sanctions listings, and cybersecurity rankings.
10. You struggle to report on vendor risk and engage the board.

6 Problems with Manual Spreadsheet Based Third-Party Risk Management Processes

While manual processes & spreadsheets for third-party risk management are a logical place to start for smaller organisations, but as your supplier base & vendor network grows and expands so too does the need for more complex mapping, automation, and reporting.

Let's explore some of the problems organisations begin to face when using manual processes & spreadsheets for third-party risk management.

1. Lack of Data Governance

Vendor risk assessments, questionnaires, and surveys rolled out using manual processes can cause a multitude of problems. Firstly, there is a lack of data governance when using paper documents or forms that are completed manually using Microsoft Word or Excel. This can result in inconsistently entered information, missing fields, and extra work with employees having to manually key findings into a consolidated spreadsheet.

Often organisations roll out regular surveys & questionnaires – either to their employee base to see how the vendor is performing, or to the suppliers themselves to get an overview from the vendors perspective. Rolling out questionnaires & surveys using spreadsheets, email and word documents or using online tools like 'survey-monkey' can cause problems with the quality and consolidation of data, causing copious admin and data input tasks that are prone to error.

It can be challenging to implement rules around the formatting of data in excel, resulting in inconsistently formatted information that becomes a nightmare to report on later down the line. Moving to a GRC software solution to manage TPRM is a good way to significantly improve data integrity - resulting in seamless reliable reporting.

2. Too Much Manual Work

Risk teams often end up with the manual task of inputting data from risk assessments, surveys, and questionnaires into a central location. Not only do the manual processes lack data governance, resulting in inconsistent information & missed fields, but further errors can happen when data is transferred or re-entered. This arduous transfer of data takes critical time from risk teams who should be spending their time analysing data to make decisions to reduce risk.

Using spreadsheets also causes more manual work for risk teams when it comes to reporting. Reports need to be created manually, which involves arduous cross-checking against multiple data sources - taking up valuable time from risk professionals and only providing a moment-in-time snapshot of data that lacks the ability to drill down into the finer details.

3. Data Security Issues

Managing your library of vendors using spreadsheets and manual processes can cause a wealth of security problems. Multiple employees accessing the same document can cause information and documents to be overwritten. Manual processes lack data governance, resulting in poor quality data and even poorer reporting. Most manual surveys and questionnaires also lack data security and privacy and don't have the option to be anonymous when needed.

There are often problems regarding user permissions when using spreadsheets, and it can be difficult to hide certain confidential or sensitive data and financial information that forms part of many vendor-risk profiles. Even the location where documents are saved can cause problems, with some employees being unable to access certain drives and file locations. It only takes one employee to mess up a formula or click 'save as' and start working on their own version of the file for things to get out of hand.

4. Lack of Automation

Manual processes lack automation. Risk assessments that are sent out manually lack visibility of when they were sent, who they were sent by, and when they are due, making it hard to get visibility of the current status. Outstanding actions would need to be chased up manually causing additional work for risk teams. It can be challenging to set up controls and KPI's relating to each supplier when using manual processes as this requires integrations with other systems and data sources and Excel doesn't cater for the extensive mapping needed. This leaves risk teams with a lot of manual work - checking data within other systems and documents to build a complete picture of the performance of each vendor.

Without automated workflows to formalise sign off processes, send risk assessments, and implement risk treatment actions these things must be done manually, with risk teams, sending emails for approval and chasing late forms themselves. Approvals would also need to be done on an ad hoc basis via email with no formal online approval process - slowing things down and leaving teams searching through emails for proof of sign off later down the line.

5. Limited Reporting

When using manual processes & spreadsheets reporting becomes a challenge. Creating manual reports takes time, meaning, by the time the reports are created the data may have changed, leaving leaders with outdated reports that only provide a moment-in-time snapshot. Building manual reports in Excel and PowerPoint takes critical time away from risk managers who should be spending their time analysing the data to make process improvements to reduce risk. It can also be difficult to drill down into manual reports and get the level of granular detail needed to identify problems.

6. Inadequate Integrations with Other Systems & Data Sources

Using Excel & manual processes makes it complicated to integrate your third-party risk programme with other systems & data sources - without complex formulas and algorithms. This complexity makes it challenging to track KPI's & KRI's - as teams are unable to set automated rules based on data in other systems. Therefore, checks must be done manually which is time consuming and subject to human error. Many organisations also find it beneficial to pull lists from their active directory into their TPRM solution to assign owners to risks and vendor relationships – but spreadsheets are not built to offer that kind of live data mapping.

8 Ways GRC Technology Can Automate Third-Party Risk Management

Managing third-party risk is a common problem faced by businesses which is why there is a range of GRC technology solutions available to support organisations to manage this critical area. These GRC tools bring third-party risk management online, automate processes and offer best-practice workflows, system integrations, and mapping - to allow organisations to get the holistic view of risk they need to make critical decisions.

Let’s explore how GRC software transforms third-party risk management:

1 Building a Centralised Register of all your Third Parties

Housing your central register of third parties within a specialist GRC tool has countless benefits. Firstly, it is much simpler to collect the data from the stakeholders that own those supplier relationships across the organisation. Staff simply complete an online form to log a new supplier within the system and staff can complete the relevant details. The solutions often come with out-of-the-box best-practice forms ensuring the data is captured consistently, and risk teams can further customise the forms to collect any additional details required that are bespoke to the needs of the organisation. The online forms allow firms to set data governance rules using mandatory fields, lists, and dropdowns to ensure details are categorised & completed correctly.

The database of third parties within the solution can be linked to your employee directory via API integrations ensuring all vendors are owned by a current employee - incorporating accountability into the third-part risk management process. Best-practice third party risk solutions often allow users to upload documents and links relating to that supplier, like contracts, SLA agreements, and URL's - building a complete picture of each vendor profile. As the system becomes embedded, a complete vendor database is created with very little work from the risk team.

When entering a supplier into the system, stakeholders will be asked to input key details about the vendor including cost, length of contract, SLA's, KPI's, plus any Key Risk Indicators and their likelihood & criticality. Capturing this critical data within a GRC tool enables risk teams to view insightful dashboards & reports comparing the dependencies, criticality, and risks associated with each vendor. This information can be used right up to board level to understand the criticality of each supplier, helping to inform where they allocate budget & resources or cut spend. Risk can be assessed holistically within the solution and vendors become comparable - making it easy for leadership to decide which areas to allocate budget to reduce risk, and which risks they are willing to tolerate in pursuit of their business goals.

Having the risk register held digitally enables organisations to take advantages of other capabilities within the solution. For example teams can set controls to monitor risk against Key Risk Indicators and automated workflows for approvals, escalations and risk remediation.

2 Standardising the Onboarding Process

The best-practice frameworks and templates within a GRC solution let you create a standard onboarding process for all suppliers. Online customisable forms can be sent out to the internal team champions managing each supplier ensuring the information is captured consistently and centrally within the GRC platform. Stakeholders can also save contracts, and log SLA's and KPI's for each vendor within the solution. The data feeds directly from the online forms into the software platform and can easily be reported on and 'visualised' using automated reports & dashboards.

This ensures the necessary due diligence is done up front before the supplier is onboarded - preventing problems further down the line. Organisations in the vendor selection process, can use the forms & templates within the solution to build a profile of each potential vendor and benchmark them against each other to select the preferred supplier. Approval workflows to onboard new vendors, allowing senior management teams to view the stats on each vendor and select their preferred option with the approval process completely tracked online. This online vendor selection method brings risk teams into the decision-making process and highlights potential pitfalls to those selecting the vendor - that may otherwise have gone unnoticed.

3 Monitoring KPI's, KRI's, & SLAs Based on Live Data

Once each supplier has been onboarded and logged in the system and organisations have a live register of all their third parties, they can start to gather further information on each vendor. Stakeholders can log the criticality of each vendor on your preferred scale, they can define Key Risk Indicators (KRI's), Key Performance Indicators (KRI's), and SLA's. These metrics can then be digitally linked to real life information like online vendor risk assessments, questionnaires, and surveys.

Incident logs and other operational data relating to KRI's and KPI's can also be pulled into the third-party risk management solution via API integrations with other systems & data sources and linked to the relevant rules regarding KPI's and KRI's - giving clear indications of when a vendor is not performing or posing a risk. Teams will have clear visibility of which systems, business processes, individuals, and departments will be impacted if the vendor fails.

By using automated software to map processes, organisations can get early visibility of risks that would otherwise go unnoticed if left to manual processes and gut feel. A vendor's performance should be regularly checked against KPI's, KRI's, and SLA's and automated workflows & alerts can be used to perform these regular checks ensuring performance is closely monitored.

4 Online Risk Assessments, Questionnaires, and Surveys

Rolling out your vendor risk assessments, questionnaires, and surveys online using GRC software will significantly simplify the third-party risk management process. GRC software usually provides out-of-the-box templates for risk assessments that can be further customised to meet any unique requirements. These can be pushed out at an internal level to your own teams to ascertain how the vendor is performing, or they can be sent to the suppliers themselves via a discreet online portal.

The forms ensure data integrity by having strict data governance rules like dropdowns, menus, and formatting, and rules around mandatory cells - ensuring all data is captured thoroughly and consistently. Teams can also upload photos, URLs, and evidence documents to build a thorough assessment of each supplier.

Risk assessments, questionnaires, and surveys can be sent out on a regular basis using automated workflows & alerts which send links to online assessments, surveys, and questionnaires. The results are all captured in the solution as part of the vendor profile. Any late completions will automatically be chased up via automated reminders. This automation cuts out copious amounts of admin for risk teams. Information is captured in a consistent format in the central database meaning risk teams can easily run reports on the data at the touch of a button

Predefined workflows can be implemented to address any failed risk assessments, using route cause analysis techniques to work the problem through to resolution. Every action is date and time stamped and linked to the relevant user profile or supplier, enabling risk teams & management to get a complete overview of when risk assessments, surveys, and questionnaires were sent, and who they were completed by and when. Live reports and dashboards are available to track completions & progress and to detect problem areas.

The solution allows risk teams to store and retrieve evidence for each risk assessment and to easily manage assessment findings and implement corrective actions - forming a complete audit trail of events.

5 Digital Risk Register

Any third-party risk solution should have a risk register. Setting up a third-party risk register online using GRC software brings a wealth of advantages for organisations.

Out-of-the-box templates will be available to log a risk, and these can be further customised to include any additional information you need to capture. The standardised fields, menus and drop-downs ensure the accurate and consistent logging of risks. Users can categorise risks into core groups like operational risk, cyber & IT risk, ESG risk, and strategic risk or by vendor or business unit – owners can also be allocated for each individual risk or risk area. 'Key Risk Indicators' can be set for each risk; these can even be based on live transactional or operational data which can feed into the solution via API integrations with your other data sources & systems - ensuring a single source of truth. Users can enter key attributes relating to each logged risk including, priority, likelihood, impact, recommended response, risk owner and status - and management teams can then make informed decisions about if they will accept, transfer, mitigate or avoid the risk.

When using a GRC tool to host your risk register, as the data is held digitally and entered consistently, management can easily view reports & dashboards to understand which business areas are likely to face a risk related incident. These real-time reports can also be used for audit purposes and reporting to the Board. As part of your digital risk register many GRC tools also allow you to log and manage the positive upside of risk as potential opportunities - enabling leaders to make well-informed risk-based decisions.

6 Automated Control Monitoring

The critical layer of oversight and policing provided by automated control monitoring as part of a third-party risk management programme is simply not possible when using spreadsheets. Automated control monitoring is essentially a set of rules organisations can establish to look out for certain metrics in large data sets. This is particularly useful in risk management as it can be used to detect when your KRI's indicate that you are nearing your risk tolerance, it can also be set to detect anomalies in large data sets like risk assessment & survey results, and to flag missed deadlines & performance issues.

Once the TPRM solution detects that levels have reached a certain limit (based on pre-defined parameters), automatic notifications are sent to the relevant parties so a decision can be made on whether to investigate further. It is like an extra layer of policing that humans may not detect, adding another line of defence. This functionality has been widely used in large financial services institutions for decades to detect unusual transactions and is an essential layer of the third-party risk management process in mid to large organisations.

7 API Integrations

Data holds vital clues about how your vendors are performing. Whether it's the data you collect via risk assessments, questionnaires, and surveys or transactional or operational data held in other systems, data sources and spreadsheets, it can all provide vital insights into vendor performance. If you were using manual processes, it would be impossible to link these data sources to your third-party risk spreadsheet and set parameters to send notifications when data indicates that a certain level has been reached. But managing third-party risk using GRC software lets you do just that!

GRC solutions enable you to pull in data from other systems and sources into the TPRM solution using API integrations. For example, if your vendor is a courier and their percentage of deliveries drops below the required SLA, automated control monitoring of the data through APIs will notify risk teams and the supplier owner, enabling them to address the problem. Businesses also use API connections to link their TPRM database to their active directory to ensure supplier relationship owners are up-to-date, and they use APIs to pull in data around lists of sites, departments, and systems to allocate risk locations and map the business processes affected.

8 Automated Workflows & Alerts

Monitoring third-party risk using GRC software enables you to set up automated workflows & alerts for multiple scenarios - saving copious amounts of time on emails and approvals.

Workflows can be set up to onboard vendors, log risks, complete tasks & actions, and send out risk assessments, surveys, and questionnaires. All actions are logged in the system enabling risk teams to view status reports and follow up on outstanding actions. Risk teams can use workflows to schedule their monthly risk assessments for the entire year, without having to send a single email and recipients simply complete the form online. Workflows send notifications when actions are overdue and risk teams can easily view the status of all risk assessments online. This automation supports employees to get formal approval to onboard suppliers, perform due diligence, and get quick decisions.

Automated workflows cut back on huge amounts of admin for risk teams, who can then spend their time analysing the data, using the results to guide the business on how best to manage the collective risks associated with their network of vendors based on their criticality and likelihood.

How Can I Further Mature My Third-Party Risk Management Process?

Mature organisations will have an established risk universe and typically categorise risk into key areas like geopolitical, reputational, financial, regulatory, compliance, cyber & privacy, operational, strategic, digital, and business continuity risk.

They can use this same method to identify which risks should be used to evaluate third-party relationships and establish the level of risk that the organisation is willing to take. Using a standard risk model will also help organisations to classify third parties based on defined levels of risk (e.g., low, medium, high, critical).

The maturity of a third-party risk management programme increases as you collect more and more data on each supplier and use complex mapping to understand the relationships and interconnectedness between your entire network of vendors, third parties and suppliers.

To increase the maturity of your third party-risk programme, manual processes & spreadsheets will not provide the data integrations, automated monitoring of controls, complex mapping, and real-time reports needed to further mature your TPRM programme. Implementing GRC software is the logical next step.

GRC 20/20's Third Party GRC Maturity Model

Michael Rasmussen defines the TPRM maturity model as:

Strategic Process, Information & Technology Architecture Alignment

1 Ad-hoc

Organisations at the Ad Hoc stage of maturity have siloed approaches to third-party governance, risk, and compliance at the department level. Businesses at this stage do not understand risk and exposure in third party relationships; few if any resources are allocated to third party governance. The organisation addresses third party GRC in a reactive mode - doing assessments when forced to. There is no ownership or monitoring of risk and compliance, and certainly no integration of risk and compliance information and processes in context of third party performance.

2 Fragmented

The Fragmented stage sees departments with some focus on third party GRC within respective functions - but information and processes are highly redundant and lack integration. With siloed approaches to third party GRC, the organisation is still very document-centric. Processes are manual and they lack standardisation, making it hard to measure effectiveness.

3 Defined

The Defined stage suggests that the organisation has some areas of third-party GRC that are managed well at a department level, but it lacks integration to address third party risk across departments. Organisations in the Defined stage will have defined processes for third-party GRC in some departments or business functions, but there is no consistency. Third party GRC processes have the beginning of an integrated information architecture supported by technology and ongoing reporting. Accountability and oversight for certain domains such as bribery and corruption risk and compliance, and/or information security are beginning to emerge.

4 Integrated

In the Integrated stage, the organisation has a cross-department strategy for managing third-party governance across risk and compliance. Third-party GRC is aligned across several departments to provide consistent frameworks and processes. The organisation addresses third party GRC through shared processes and information that achieve greater agility, efficiency, and effectiveness. However, not all processes and information are completely integrated, and there is not an integrated view of third party performance.

5 Agile

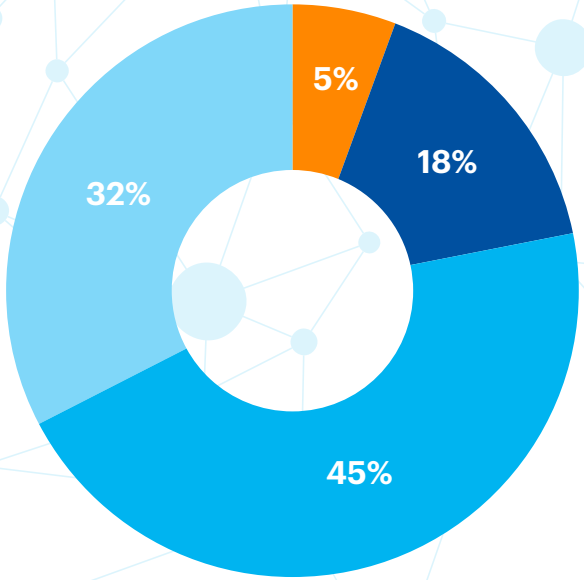
At the Agile Maturity stage, the organisation has completely moved to an integrated approach to third party GRC across the business that includes an understanding of risk and compliance in context of performance and objectives in third party relationships. Consistent core third party GRC processes span the entire organisation and its geographies. The organisation benefits from consistent, relevant, and harmonised processes for third party governance with minimal overheads.

Issue to Departments to Enterprise Coordination and Integration

How Do Organisations View Their Third-Party Risk Maturity?

A recent Deloitte survey indicated that only 23% of organisations view their third-party risk management maturity as Integrated or Optimised. While 77% still felt like they were in the Initial or developing stages of setting up their third-party risk management programme, indicating that organisations have a lot of work to do to improve in this area.

Organisational Maturity in Integrated TPM: Overall, by Industry and Geography



- **Initial:** Most third-party management processes embedded in functional domains with limited integration/connectivity across applications.
- **Developing:** Some alignment and coordination across specific third-party management processes, often by stitching together base applications in ad-hoc ways.
- **Integrated:** Third-party management processes aligned and coordinated across the entire organisation.
- **Optimised:** In addition to being integrated, process performance is continually improved through incremental and innovative technological enhancements.

As you think about the current state of your third-party risk management programme, consider where you are on this maturity model and what steps you would need to take to further mature your programme. If you have reached the limit of what spreadsheets can offer, it might be time to consider a purpose built TPRM software solution to escalate and mature your programme.

For those that already have the fundamentals in place and are using GRC software to manage third-party risk, you might want to consider taking some of these additional steps to further mature your programme.

8 Ways to Take Your Third-Party Risk Management Programme to the Next Level of Maturity

1

Link Live Transactional and Operational Data to Your Third-Party Risk Programme

As part of a third-party risk management programme, most organisations will set KPI's, KRI's and SLAs for each vendor and try to monitor this on an on-going basis. As part of this setup an organisation will define which data & metrics these will be based on, for example this might be data from sales, finance, incident reporting, HR, IT, or operations. Risk Teams will devise a rating scale and set rules and parameters to define what constitutes good and bad performance or risky behaviour based on the data available to them.

In manual third-party risk management programmes, risk teams will often request performance data and risk assessments, surveys, and questionnaires from different teams around the business to try and build a picture of how the vendor is performing. Often the information needed is stored in other systems, spreadsheets, and databases across the organisation. This makes the task of cross checking KPI's, KRI's and SLA's a manual, time consuming task for risk teams.

GRC software can greatly simplify this process by pulling in live transactional and operational data directly into your third-party risk programme through a series of API connections to your other data sources. Pulling this data directly into a TPRM programme enables teams to monitor vendor risk & performance based on live data. The automated functionality within GRC software enables users to set up controls based on live data, therefore if metrics reach a certain level indicating risk or poor performance, automatic notifications are sent to the relevant stakeholder, and if they don't act, automated reminders will be sent. Users can also update any actions & progress into the solution, keeping a full audit trail of all problems and the response.

2 Dependency Mapping

Most vendors don't perform one isolated function within an organisation. If a vendor is performing poorly or is unable to provide their goods or service, it is helpful to know which teams, departments, business processes, and other vendors will be affected and how critical that would be. This also helps risk teams further understand the criticality of each vendor.

Using spreadsheets does not allow for the extensive mapping required. But organisations who use GRC software for third-party risk management can take advantage of the extensive mapping capabilities available. By storing all their business processes, teams, and departments in your GRC tool (these can usually be pulled through using API connections to HR systems etc) they can easily map vendors to the business processes and teams directly affected by their performance. This gives any indirectly related teams insight into vendor performance and the associated risks. Once the key areas are mapped, controls can be set to notify relevant stakeholders of any supplier issues that could have an impact on their department.

3 Automated Approval Workflows

To get a comprehensive third-party risk management programme it is best to involve as many stakeholders in the process from across the business as you can. This means granting access for employees at all levels of the organisation to log a new vendor or log and track a potential risk. It is best to implement an approval chain when opening up the third-party risk management process to multiple users to ensure there are no duplicates or unnecessary details added.

Managing third-party risk using a specialist GRC software tool enables risk teams to set up automatic approval workflows, enabling employees to log new vendors & risks and get instant approval from line management. Notifications are automatically sent when a new risk or supplier is logged and once approved the individual who added the details will be notified. This adds a layer of policing without slowing down the process and enables more employees to feed into the vendor risk management programme providing risk teams with more data and insights.

4 Linking Incident Management to Third-Party Risk Management

Mature organisations realise that their incident log should be linked to their third-party risk management programme. Risks could perpetuate into full blown incidents, and a high number of incidents in a certain area could signify a potential risk that needs to be added to the risk register and managed. Many organisations also use their incident log to pull data about certain supplier related incidents into their TRPM solution to build a better overview of how that supplier is performing.

To link these 2 functions requires complex mapping and that's where GRC software can support organisations. Most GRC software solutions offer incident management and risk management capabilities in the same platform. This enables your entire incident log to feed into your third-party risk management programme – providing vital details of any incidents caused by each supplier. Risks that turn into actual incidents can be quickly converted into an incident with a full audit trail to see when it was escalated and by who. Similarly, risk managers can run reports on the incident log to ascertain if risks should be added to the risk register. This comprehensive approach builds a more complete picture of vendor performance enabling risk teams to see the bigger picture. Many incident management tools also enable teams to log near misses, these can also be added to the risk register.

5 Online Portal

Many GRC software tools offer online portals to capture external or anonymous information. This is a great way to roll out vendor risk assessments, questionnaires, and surveys to your suppliers. They simply complete the forms online, and all the data they entered feeds directly into your third-party risk programme. This saves copious amounts of admin time for risk teams who can then focus their attention on analysing the data and advising the business on the best course of action.

These online portals are also a good way to do anonymous reporting from any internal employees, especially regarding sensitive information like whistleblowing. Employees simply input the data into the portal, giving risk teams undercover insight into what is really happening in the business.

Links to the online portal are usually sent out via automated emails from the GRC software platform - using automated workflows to trigger the email sends.

6 Linking Compliance Obligations to Your Third-Party Risk Programme

Many organisations like their vendor network to uphold many of the same ethical values and standards as their own company. That's why more mature organisations choose to map compliance obligations to their vendor database. You may wish for your suppliers to be GDPR compliant or meet certain ISO standards and require proof, or you may wish for vendors to follow some of your own internal policies & procedures. This should all be tracked - and score carded as part of the vendor profile within your third-party risk management programme.

GRC software tools that offer third-party risk management solutions and compliance capabilities in one platform can support an organisation to set up this complex mapping of requirements. This enables organisations to get a clear view of which of their third parties is compliant with required regulations, legislation, and internal policies and procedures.

7 Linking Third-Party Risk to Health & Safety

Health & safety is another discipline that many organisations choose to incorporate into their third-party risk programme. If vendors are causing health & safety incidents or you want them to follow certain safety protocols or operate in line with ISO14001 and other safety standards - this needs to be tracked and monitored as part of their vendor profile.

Best-practice third-party risk software solutions that offer health & safety, incident management, and compliance in the same platform as the third-party risk functionality are an ideal choice for organisations who want to incorporate health & safety requirements into their vendor risk programme.

8 Linking Third-Party Risk to Business Continuity Planning & Operational Resilience

Organisations work with a network of suppliers & vendors for good reason, they provide vital products, raw materials, and specialist services & technology that the business can't operate without. That's why many organisations choose to integrate third-party risk management with their business continuity plans and operational resilience goals.

Businesses realise that they must have a contingency plan in place in case any of their suppliers can no longer deliver their product or service. That's why linking business continuity planning and third-party risk management is a logical next step for organisations looking to further advance their TPRM programmes. GRC software that offers BCM capabilities in the same platform as third-party risk will enable organisations to map their business processes, systems, and people to both their vendor database and their business continuity plans, providing vital visibility of the dependencies of each supplier and any back-up plans & alternatives.

Engaging the Board in Third-Party Risk

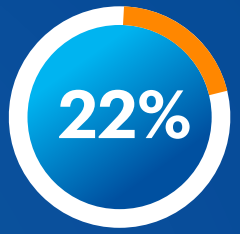
Board members and senior decision makers must be engaged in the third-party risk management process. After all, it is the leadership team who often allocate the budget for each vendor and have the authority to take it away. The reputation of the entire business could be on the line if a vendor performs badly and negatively impacts the company or provides poor customer service.

It would not be helpful for the board to hear about each vendor in an isolated context as there would be no way to compare or benchmark the vendor against other suppliers, third parties, and business partners. Boards will find it more engaging if they can directly compare vendors in terms of cost, performance and inherent risks and build an understanding of the dependency on that vendor from other suppliers & departments. That's why getting a centralised view of third-party risk is becoming a hot topic, even at board level.

The best way to engage the board is through transparent reporting on real performance data. That's why it is so important to feed live data into your third-party risk programme. Viewing reports on current performance and getting visibility around the status of KPI's, KRI's, and SLA's is essential for board members. This needs to be shown in the context of spend, criticality to the business, and impact on revenue - to ensure the supplier is still a viable option and is not causing undue risk to the organisation.

According to recent research by KPMG

of third-party risks are classified as critical or highest risk.



of respondents report breaches to their board.

Manual spreadsheet-based approaches become unmanageable when trying to report to the board, as they simply don't offer the complex mapping needed to present adequate data with the option to drill down into certain areas to view the finer details.

Organisations using GRC software for third-party risk management find it much easier to engage the board. It takes them much less time to prepare for meetings - as most reports can be produced at the touch of a button - and metrics are always based on the latest data within the tool. GRC tools provide risk teams with in-depth analysis - enabling them to provide a more holistic view of risk that can be used to support the board to make critical decisions on budgets, spend, and resources.

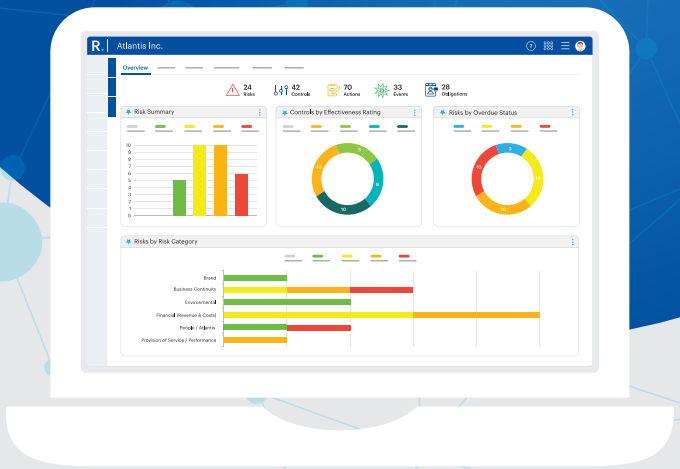
The live reports & dashboards available to risk teams within a purpose-built third-party risk management solution also enables them to identify problems quickly. This empowers them to approach the board on an ad hoc basis to address any likely risks or performance issues before they escalate into full blown incidents. The data also helps them to weigh up risk versus reward - enabling them to guide strategic decision-making.

Unlocking Opportunities Through Third-Party Risk Management

A good third-party risk management programme is not just about mitigating risk, it is also about understanding the overall performance of each vendor and recognising opportunity. If a certain supplier is performing well, you might want to outsource more work to them to improve business performance. If switching to a different vendor means you can get the same product or service at a fraction of the cost, use your third-party risk management process to investigate the opportunity and understand the risks involved.

A good third-party risk management programme will enable risk teams to understand potential business opportunities by partnering with certain suppliers. These opportunities should be captured as part of the vendor scoring process and further investigated in areas where the opportunity outweighs the risk.

Ready to Move to an Automated Third-Party Risk Management Solution?



Could your third-party risk management process use some TLC? Do you like the sound of online risk assessments, automated workflows & alerts, and instant reports & dashboards? Talk to the Camms team about how we can help to add structure & automation to your third-party risk programme and integrate it with other core GRC processes.

The camms third-party risk solution enables you to build a dynamic vendor register and log any associated risks. Teams can roll out vendor risk assessments, questionnaires, and surveys online - with results feeding directly into the solution. The solution enables you to define KPI's, KRI's and SLA's and monitor progress using automated control monitoring.

Camms offers a cloud-based SaaS GRC solution that aligns with your organisational strategy, so you can manage third-party risk as part of a holistic GRC programme linked to your strategic goals & objectives. The solution uses a modular approach, allowing organisations to scale and mature their GRC programmes and strategic planning at their own pace.

Check out some of the other core capabilities within the Camms solution:

Risk Management

Set up a comprehensive risk register, track progress, and define KPIs and tolerances based on your risk appetite. Use the structured framework to define ownership and set key risk indicators, use automated workflows & alerts to flag problems, and implement structured approval processes.

Compliance Management

House a comprehensive obligations library of relevant regulations, legislation, policies, ISO standards, and internal procedures - and ensure compliance. Set a structured process for version control, approval, ownership, and regulatory change. The solution integrates with third-party regulatory content providers to offer regulatory horizon scanning.

Governance

Implement workflows, registers, and sign-off procedures for any process – including safety checks, feedback & complaints, disclosures, inspections, whistleblowing, questionnaires & surveys.

Strategy Management

Break down your strategic goals & objectives into lower-level projects & tasks and allocate them out across the organisation to easily monitor performance and track progress.

Incident Management

Facilitates incident and near miss reporting in real-time and triggers the investigation process post-event.

Audit Management

Schedules and manages internal & external audits and formalises the results and required actions.

Cyber & IT Risk

Manage the complex framework of compliance requirements and risks related to ISO standards and data privacy laws like GDPR.

API Integrations

Transfer data from other systems in and out of the Camms solution via API connections, enabling you to base KPIs on live data.

Stakeholder Dashboarding

Intuitive functionality provides executives and the board with key risk, compliance, and strategic progress information when required.

Analytics & Reporting

Built-in dashboards & standard reports provide critical risk insights and executive reporting that satisfies requirements from auditors & regulators.

Managing these different functions in a centralised platform fosters collaborative working and the sharing of data across teams. It enables communication from the top-down and bottom-up and ensures operations follow best practice processes to keep leaders, auditors and regulators satisfied.

Discover How Camms is Helping Organisations to Improve Third-Party Risk Management

Camms offers a cloud-based SaaS solution that provides a best-practice framework to manage third-party risk.

Build a vendor database, create a vendor risk register, and roll out vendor risk assessments, questionnaires, and surveys online. Use automated control monitoring to track performance against KPI's, KRI's and SLA's and view reports & dashboards at the touch of a button

Integrate risk management with compliance, strategic planning, incident management, audit management, and operational resilience planning - to form a complete end-to-end solution.

With integrated solutions across governance, risk, compliance, ESG, strategy, and project management, Camms software is helping organisations manage risk, make the right decisions, and streamline and automate processes.

Request Demo **Visit Website**

Camms.

Software to change tomorrow.