

THIRD-PARTY RISK MANAGEMENT

Strategies to Maximise Value
And Minimise Risk





Contents

Introduction	1
What is Third-Party Risk?.....	2
The Rise and Rise of Third Parties.....	2
Why is Understanding Your Third Parties Important?.....	2
Third-Party Expansion and Blind Spots.....	3
Third-Party Risk Management.....	4
The Third-Party Risk Landscape.....	5
Understanding and Protecting the Value of Data	6
The Foundations of a Strong Third-Party Relationship	8
The Vendor Management Life Cycle.....	9
Third Parties and Your Business Continuity.....	13
15 Third-Party Red Flags.....	14
Third-Party Risk Management Maturity.....	15
Helping Third Parties Understand Their Gaps	16
Taking the Next Steps to Enhance TPRM Maturity.....	16
Fast Tracking Third-Party Risk Management.....	17
How Can We Help?.....	18
Appendix 1 – Vendor Cyber Risk Posture Report.....	20
Appendix 2 – Third-Party Review Checklist.....	22
Appendix 3 – Express Cyber Risk Questionnaire.....	23
Appendix 4 – Cyber Security Questionnaire.....	24
References.....	26

Introduction

Today, it is hard to find a business that doesn't have some form of dependency on another business. That other business providing a service is often referred to as a third-party, supplier, vendor or sub-contractor depending on the nature of the business relationship, product, and service they provide.

Outsourcing of IT services gained popularity in the 1990s, but in recent years, we have seen an exponential growth in the use of third parties thanks to flexible delivery options, enhanced expertise, reduced delivery risk, greater process efficiencies and cost efficiencies that can result in a strategic competitive advantage for an organisation.

However, a number of recent adverse events ranging from severe weather events, the COVID-19 pandemic, targeted cyber-attacks, political trade wars, raw material shortages to shipping and port backlogs, have highlighted the fragility of supply chains, exposed third parties to a range of real vulnerabilities and in turn transferred this risk back to many organisations.

In one study, approximately 73% of all industries reported issues with suppliers, production and distribution.

To be successful as an organisation, you need to be willing to take, and effectively manage a wide range of risks to achieve the desired objectives.

As organisations engage with third parties either locally or internationally, the level of inherent risk assumed rapidly increases. How can you prepare for the opportunities and challenges posed by utilising third parties?

At InConsult we want you to confidently take more calculated risk.

This publication helps provide insight into strategies that can be used to confidently address and manage the risks associated with your third parties and supply chain. We offer tips and resources to help you better manage third party risks.



What is Third-Party Risk?

Third-party risk is defined as the potential risk that arises from an organisation relying on external entities to perform business services or activities on their behalf. Third-party risks can also be known as vendor risks, supplier risks or supply chain risks.

The Rise and Rise of Third Parties

While third parties can potentially increase risk, especially to the ill-prepared, they can also unlock a whole new world of operational capabilities.

The increase in dependency on third parties has very closely followed the progression of digitalisation and the boom of the Internet of Things (IoT). This is not merely referring to the dependence on digital services such as telecoms, cloud and hosting services, but rather the depth and breadth of web-based, business applications and services that IoT is empowering to improve production and output capacity.

We are no longer tied down to physical assets and local suppliers, we can choose from the best of breed and from a global talent pool of third parties.

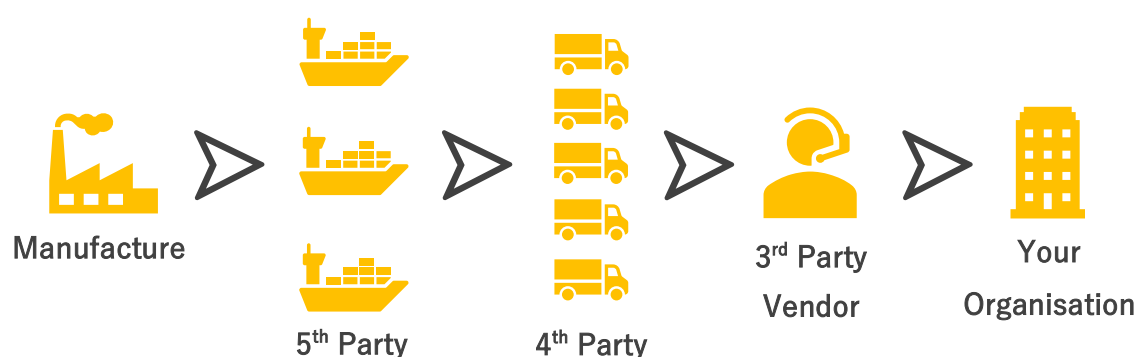
Why is Understanding Your Third Parties Important?

Businesses can have hundreds or thousands of third parties. The risks can be influenced by internal factors that impact vendor performance or external factors such as industry trends or global conflict. These internal and external factors are not static, particularly external influences and so all the risks relating to third parties are constantly evolving and must be reviewed and monitored regularly.

Third-Party Expansion and Blind Spots

There is a strong trend toward an increase in the use of third parties at an abnormally rapid pace. Third parties have a high probability of involving fourth parties, fifth parties and so on, to provide a product or service to a client.

If we consider these parties as networks, ultimately a vast array of networks across multiple continents are the foundation of a client-facing conglomerate. As the costs of manufacturing and services overseas are often lower and more competitive, the scales are heavily tipped towards outsourcing and a long list of distributors that act as the translators.



3 in 4 Chief Procurement Officers cannot confidently predict risks within their supply chain, issues with suppliers, production, and distribution.

Considering this chain of networks, it is very likely that a third-party is not the end of the line. These vendors may even provide more than just a product, such as being the “middle-man” to a manufacturer while also providing a mediating service like technical support, warranty, and claims. Fourth and fifth parties are potential risk blind spots.

Overall, there is great benefit when the right “network” is selected as quality can be assured, costs can be reduced, and profit margins speak for themselves. It is a reasonable choice to rely on these parties but at what point do we determine that the risk is too great and how might these risks change over time as the vendors evolve?



Third-Party Risk Management

Third-Party Risk Management (TPRM) is the process of assessing the *ongoing* risks associated with using third parties in your organisation. It involves obtaining a sound understanding of the risks associated with each third-party and service provider and requires scanning, obtaining current information, monitoring, controlling and regularly reviewing the many potential risks.

Third-party risk management aims to reduce unnecessary risks and costs associated with third-party related risk exposure. In other words, TPRM aims to reduce the chance of operational failures, protect sensitive data, meet regulatory and contractual obligations, and to ensure both organisation achieves their desired objectives in the relationship.

To be effective, TPRM must consider a wide range of risks, such as ethical business practices, financial stability, corruption, environmental impact, modern slavery considerations and information security procedures.

The necessary due diligence must be in place to review all of these areas before a third-party can be onboarded to ensure risks are identified, understood and adequately controlled. Beyond the initial due diligence, ongoing monitoring is critical.

The Third-Party Risk Landscape

Much like the internal risk landscape, the third-party risk landscape can have just as equally devastating consequences on a business if its not well understood and managed.

- **Operational Risk:** The risk of loss resulting from inadequate or failed processes, people, and systems or from external events effecting the third-party. A third-party falling victim to a cyber-attack, supply chain disruption, trade war or natural disaster could cause a system failure that temporarily disrupts your business.
- **Transactional Risk:** This is a form of operational risk. It is the risk arising from problems with service or product delivery. A third-party's failure to perform as expected due to reasons such as inadequate skills, technological failure, human error, poor training, inadequate staffing, or fraud, exposes your organisation to transactional risk. These issues could result in unauthorised transactions or the inability to transact business as expected.
- **Regulatory/Compliance Risk:** The risk arising from a third-party's violations of laws, rules, or regulations, or from non-compliance with their internal policies or procedures or non-compliance with your organisation's policies or ethical standards.
- **Financial Risk:** The risk that a third-party, under financial stress, is no longer financially viable and is unable to meet the terms of the contractual arrangements.
- **Cyber Risk:** Third parties are often the favoured vector for cyber-attacks today. Attackers infiltrate supply-chain links, silently infecting their systems and devices. The attacker then uses the third-party as a "platform" to launch attacks on higher-value targets including customers.
- **Reputational Risk:** The risk of negative public opinion originating from an adverse and/or highly publicised incident that ranges from a security breach, violation of the law, to poor customer experience. Reputational risk can have a knock-on effect on your organisation, i.e. you may be targeted by association. Reputational damage is difficult to anticipate and measure, which makes robust risk assessment, due diligence, and monitoring critical.
- **Strategic Risk:** The risk of misalignment between the third-party and your organisation's business strategies. Misalignment can result in poor business decisions or changes made by a third-party that impact your organisation negatively.



Understanding and Protecting the Value of Data

Most third-party risks have been well understood and managed fairly to varying degrees for many years. But the newest and more complex risk relates to cyber security and the privacy of data. The value of data held by third parties is often not well understood and managed. This area needs special attention.

- Depending on your business, the location of customers and industry, the data protection and privacy laws will vary. We recommend working to the highest standards and compliance obligations relevant to your organisation.
- Define the appropriate level of cyber security and data protection policies and practices that your organisation will aim to achieve internally. This now also sets the minimum standard for your third parties.
- Identify all your third parties. This can be a real challenge as not all third parties are centrally managed by procurement or information technology. Communicate your standards to your third parties and build minimum cyber security and data protection standards into contracts.
- Establish a data inventory or information asset register to understand what type of sensitive data your organisation has and who has it. This helps identify all systems and third parties who can access, store, process, distribute and/or transfer data on the organisation's behalf.

- Using web-based questionnaires, gather information from your third parties about their cyber security, privacy and data protection posture. The type, size and complexity of the questionnaire should change with the level of risk of each third-party.
- The questionnaire can also be strengthened by powerful web-based predictive analysis of many risk factors including email security, SSL, DNS health, open ports and common vulnerabilities. If you can, set up automated alerts for high-risk third parties for continuous monitoring.
- Once the results are in, perform gap analyses and benchmarking across your third parties to assess the current state of cyber security and data protection practices.
- Start a conversation with your third parties about their security posture focusing on the high-risk areas. Provide them with suggestions and realistic timeframes to help build positive relationships.
- Repeat the process at least annually to monitor commitment to improvement or new weaknesses. Higher risk third parties will require more regular attention.

The Foundations of a Strong Third-Party Relationship

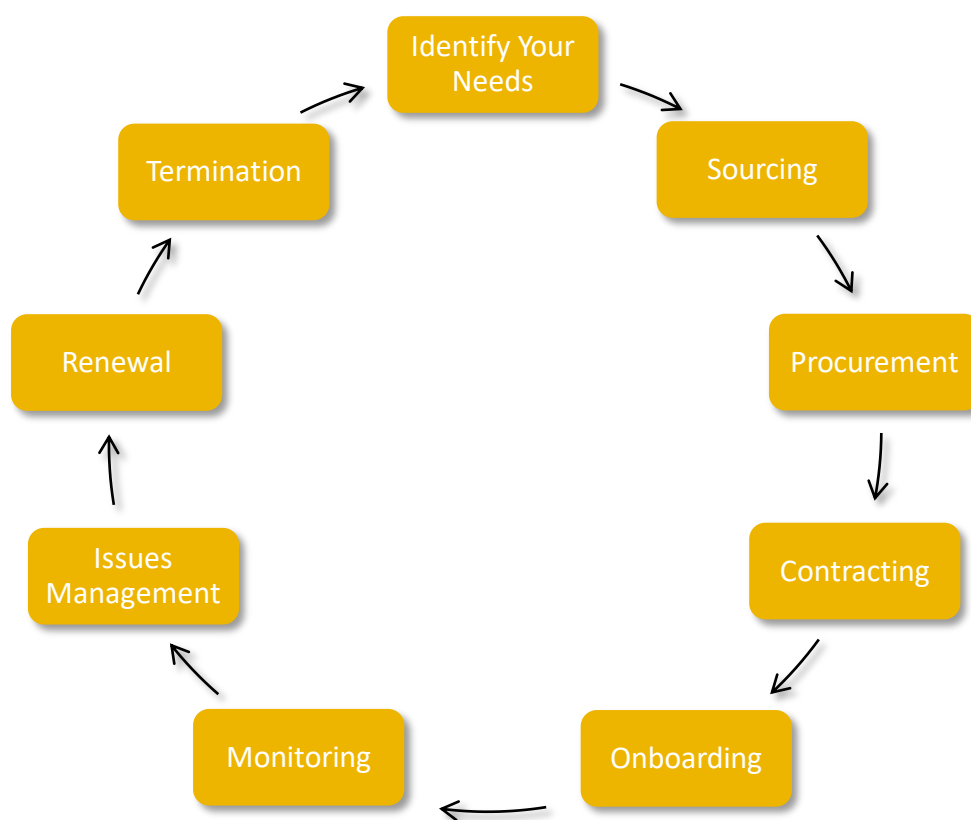
Taking the Third-Party Risk Landscape into consideration, it is easy to understand the potential risks at a high level and what needs to be put in place to avoid them. Like any business relationship, a successful third-party relationship relies on these important components to help manage those risks:

- **Open communication:** Open communication starts from the request for tender or proposal requirements and should thrive throughout the relationship. It requires both parties to be open and honest about their expectations and requirements (buyer) and capabilities (third-party/supplier).
- **Knowledge sharing:** Research shows that knowledge sharing can increase supply chain efficiency by reducing inventories and smoothing production. Supply chain efficiency is highly important as today's competition is no longer between companies, but between supply chains – therefore an organisation linked to a more efficient supply chain than its competitor will have an advantage.
- **Service agreement:** Service agreements are used to define services, expected service levels, responsibilities, timeframes, payment, pricing and measure the performance of the third-party. A good service agreement is fair and not weighted to one party, defines clear expectations and key performance indicators, and considers cultural and ethical norms of both parties. Ensure that all service agreements cater for meeting a range of regulatory obligations that can apply to third parties. For example, the Australian Prudential Regulation Authority (APRA) has several prudential regulations that require organisations to have a deep understanding of outsourced activities around sensitive information, disaster recovery and security.
- **Regular performance review:** Monitoring third-party performance not only reduces service problems and failures, but also keeps the relationship balanced and helps align the goals of both organisations. The frequency of performance reviews should be based on the risks associated and materiality of the third-party.
- **Periodic thematic assessments:** A growing trend is to ask third parties to complete a range of thematic assessments relating to information security, business continuity and other areas of compliance such as modern slavery. Periodic assessments provide insight into the commitment and growth of third parties. They are key to maintaining open communication, ongoing knowledge sharing and assisting with performance reviews.

The Vendor Management Life Cycle

The vendor management life cycle is a better practice, end-to-end approach of how organisations should manage third parties and external entities in a proactive, structured, and transparent manner.

Adopting the lifecycle is a great start to managing the third-party risks. There can be minor variations to each element of the lifecycle, but typically it includes the following areas:



Identify Your Needs

The process starts with you. When you recognise the need to outsource an activity or engage an external entity or third-party, the first step is to define your needs. Your needs should be clearly identified, documented, and approved by management and the governing body where appropriate. The key controls here include well-documented requirements, a sound business case, a risk assessment, defining expectations, and extensive stakeholder engagement.

Sourcing

Once you have a good understanding of your internal needs, start looking externally to the options available. The sourcing of potential third parties involves conducting research to identify a pool of potential vendors or narrowing potential vendors down to a manageable number of options.

The methods of sourcing third parties can include word-of-mouth recommendations, prior experience with a vendor, research, prequalified buying panels or industry trade shows.

Procurement

Procurement is the process of evaluating, choosing and acquiring the goods, services, or works from a third-party often via a direct approach, tendering or competitive bidding process. Procurement is an effective way of narrowing down potential sources to those that very closely align with your requirements. It also aids the process of developing transparency.

Contracting

The contracting phase is the transferal of your expectations, specific vendor requirements, access control, information privacy and much more all combined into an agreement. What fails to be clearly defined at this stage is a mutually agreed review interval. This should not be confused with a contract renewal interval. While ad-hoc reviews are encouraged and allow for complete transparency, an agreed annual review is also beneficial as it sets a milestone for organisations and their vendors to plot a continual improvement program.

Whilst the terms and content of a contract will vary depending on the nature of goods and services, as a minimum, a contract should include:

- The scope of the arrangement.
- Commencement, end and renewal dates.
- Review provisions including compliance with unplanned reviews.
- Pricing and fee structure.
- Service level and performance requirements including audit and monitoring.
- Continuity guarantees including sub-contracting and insurances.
- Privacy and information protection requirements.
- Default, dispute and liability terms.

Onboarding

Well defined access controls are critical to reducing third-party risk. The onboarding process should reflect a 'least privileged' access control methodology for all vendors. If an incident were to ever occur, the priority should be preservation of the organisation's information or property, followed by a contingency plan. This phase is also useful when onboarding remotely as a means of validating the consistency of information technology security measures implemented by the vendor.

Onboarding allows for the configuration and implementation of processes to streamline the interactions with a vendor. Purchases are simpler, orders are clear and concise and response times should never be a topic of concern. During configuration and implementation, the organisation can exploit the transparency of the process by vetting the vendor's structure against best practice and regulatory requirements.


Monitoring Ongoing Performance

Your needs will evolve and change overtime and it is important that third-party vendors continue to meet your needs. Whether it is performance-based factors or continuity of service expectations, monitoring should be ongoing with better practice suggesting annual reviews at minimum.

Following onboarding it is critical that third parties are regularly assessed and actioned accordingly. No matter how positive the rapport is with a vendor, expectations should be set from the very start as part of contracting. This includes early expectations of business continuity documentation and staff training, and information security measures to protect your data. Early adoption of monitoring prevents vendors likening the process to unfair scrutiny or bias.

The depth of monitoring is based on the inclusions of the contract. In instances where a contract does not include remediation steps or involvement by the organisation in response to vendor shortfalls, it is considered one-way monitoring. Two-way monitoring, which should be the standard for any organisation, allows for reporting and tracking of changes made in response to monitoring.

Given that some vendors can also expose you to higher cyber risks, monitoring their cyber security posture through questionnaires and cyber security monitoring tools and then providing them with feedback is critical.

 **Appendix 1 – Vendor Cyber Risk Posture Report** template for guidance in presenting cyber related issues, gaps, findings and expectations.

There are some valuable KPIs that vendor monitoring should be based on:

- Ability to fill orders/deliver service on time and with accuracy.
- Ability to comply with organisation's terms and conditions.
- Ability to comply with legal, manufacturing, health and safety and security requirements.
- Ability to provide consistent acceptable quality with reasonable adjustments to pricing structures.
- Ability to prove ongoing review and enhancement of business continuity and security practices.
- Ability to respond to issues in a timely manner.

Issues Management

Issues management is a particularly important projection of monitoring in the real world. While it is a two-way street, a third-party should see issues as an opportunity to show commitment to the business in rectifying them promptly. This process compounds transparency and helps in the development of communication between the third-party and the business.

The business is responsible for managing third-party relationships as part of the procurement process. While it should equally work in fairness to do what is required to resolve any issues, most issue resolution will originate from ongoing monitoring. These issues can be identified by monitoring changes to the third-party organisational structure, legal actions, regulatory issues, financials, performance, business continuity controls, ethics, information security and more.

Re-evaluation/Renewal

The re-evaluation or renewal phase of the vendor life cycle is the culmination of all findings from monitoring and issues management. When the time comes for a contract renewal, the findings provide complete truth in the performance of the third-party and allow for judgement that is not influenced by sales tactics and marketing that tend to increase around a renewal date.

Be wary that some vendors may only invest interest in the relationship shortly prior to and after a renewal date. If their performance is poor and a new tender will be difficult to turnover before contract expiry, consider negotiating a shorter renewal period to offset the tender process.

 **Appendix 2 – Third-Party Review Checklist** for areas to monitor regularly.

Termination

As difficult as it is, termination is a reality. No matter the history of a relationship, a third-party performing poorly could expose the organisation to costs or damages beyond your risk appetite threshold. Once an alternate vendor has been sourced, the termination of an existing vendor must be carefully executed to ensure the offboarding considers decommissioning access and upholding information security throughout.



The transfer of information during offboarding is particularly risky as often it includes the transfer of stored or archived data from the commencement of the relationship to the end date. Once all requirements are met contractually, external access should be completely removed to ensure no malicious or unintentional acts are performed.

Third Parties and Your Business Continuity

Even with the best risk management processes and controls, things can still go wrong. It is important that each third-party have a business continuity plan and other important response plans in place.

As part of best practice, an organisation should annually review its Business Continuity Management Framework to clearly identify the most prominent critical business activities. By determining which vendors are critical, what contingencies are available and what alternate vendors can be utilised while in crisis mode, an organisation is better prepared than simply relying on the vendor to get their act together.

As a sub-set to business continuity, and one of the hottest topics for board members in the current environment, is information security. A third-party should be annually reviewing their Information Security Framework, including provisions for cyber security risks and independent audits to validate sufficient risk mitigation.

-  **Appendix 3 – Express Cyber Risk Questionnaire** to send to key third parties who have sensitive data.
-  **Appendix 4 – Cyber Security Questionnaire** to send to IT vendors who provide your business with information technology services.



15 Third-Party Red Flags

It is important that organisations conduct regular and sometimes, continuous monitoring of their third parties. Red flags are often early warning indicators to potentially larger problems. Some red flags to watch out for include:

1. The inherent risks within the region, country, or industry in which the third party participates has a history of corruption or geo-political issues.
2. Third-party contract has little detail regarding the work being performed or service provided.
3. Third-party rejects important contract management clauses like the right to audit or provide reasonable information on request.
4. Failure to provide timely or honest information during the due diligence process.
5. High turnover of key third party staff and management including account manager.
6. Frequent change of business ownership and/or business model.
7. Lack of engagement by third party to understand and meet your needs.
8. Failure to complete third party questionnaires.
9. A very poor or declining cyber security rating.
10. Failure to remediate concerns, issues or gaps raised by your organisation.
11. Unclear or overly complicated organisation or legal structure.
12. Request unusual transactions, payments in advance or abnormal contract terms.
13. A lack of established organisational policies, codes of conduct or practices that promote ethical values.
14. Inadequate insurance cover.
15. A recent spate of incidents, issues and breaches including internal tampering or theft.

Third-Party Risk Management Maturity

Risk management maturity models have been used for over 20 years and can help organisations to see where they are now and where they want to be in terms of risk management maturity across a range of important elements.

The maturity of third-party risk management can also be assessed using contemporary risk maturity assessment models, but it will require some adaptation to enhance context and value.

Most maturity models rate maturity on a scale from 1 to 5. The lower the number the less mature.

1. Initial → 2. Defined → 3. Managed → 4. Integrated → 5. Optimised

An example of the elements or attributes that are typically assessed include:

- Risk Governance & Oversight
- Organisational Policies
- Business Processes
- Tools and Technology
- Risk Reporting and Metrics
- People and Organisation Capability
- Risk Culture

Helping Third Parties Understand Their Gaps

Reporting gaps to a third party may be welcomed or it may be shrugged off as another costly venture that chips away at the relationship.

Helping vendors to truly understand the benefits of addressing operational flaws can result in improved efficiencies with gains for both parties. To communicate gaps more effectively, ensure reporting is kept positive, with clear and concise recommendations of how to resolve them in a cost-effective manner.

Remember to use friendlier language such as “observations” in place of “flaws” and remember to integrate monitoring and communication into the relationship, with regular discussions as early as possible.

Taking the Next Steps to Enhance TPRM Maturity

The next steps to ensuring you have an adequate third-party vendor assessment program is to compare the strategies against those presented in this publication. Organisations must ask the question:

- Are the organisation’s requirements clearly defined?
- Have you recently reviewed your risk assessment process?
- Do you assess vendor performance, continuity and security regularly?
- Have you prioritised your vendors into low, medium and high risk?
- Have you automated third party risk assessments and regular reviews?
- Have you identified performance and security triggers for reporting?
- Do all vendors comply with regulatory requirements?
- Do vendor agreements protect your organisation?
- Does your organisation have contingencies in place when disaster strikes?
- Do you have alternate vendors or a diverse portfolio?



Fast Tracking Third-Party Risk Management

If an organisation falls short with any of the questions above, there is no need to panic.

Thankfully, we have the tools and expertise that allow for rapid third-party risk management assessment and remediation.

At InConsult we can assist you as much or as little as you need. You are always in control.

From online questionnaires and cyber security ratings to our proprietary online vendor risk and contract management software, we combine our tools and experience to deliver rapid results.

How Can We Help?

We understand that third-party risk management is becoming more complex for many organisations, and it can be difficult to know where to start or what to do next.

We have got you covered.



Design or enhance your third-party risk management framework

We can help design your TPRM framework so that it is aligned to your risk management framework to help ensure a consistent and risk-based approach to your TPRM program based on industry better practices.

We can perform an independent review of your current third-party risk management framework in accordance with the Institute of Internal Auditors' guideline for Auditing Third-party Risk Management and assess your TPRM Maturity.



Independent Review/Audit of your TPRM Framework and Maturity



Independent Third-Party Audits

We can perform an independent and impartial audit of your third parties to assess the level of conformity of their systems and processes to your criteria.

We can perform offsite and onsite risk assessments to gather data of each of your third parties. We can plan and coordinate third-party risk assessments from start to finish.



Third-Party, Vendor or Supplier Specific Risk Assessments



Third-Party Cyber Security Risk Assessments and Continuous Monitoring

Using the latest and best of breed technology, we can evaluate the cyber security posture of your key vendors. We evaluate the results, provide a cyber risk rating and present the gaps in an easy-to-understand report. We brief you and your vendor of all assessment findings.

Using our GuardianERM technology, organisations can conduct comprehensive risk assessments and contract due diligence for each third-party supplier and vendor.



Web-based Vendor Contract Management Software

Appendix 1 – Vendor Cyber Risk Posture Report

Provides guidance in presenting cyber related issues, gaps, findings, and expectations of a cyber risk posture review.

Cover Letter

All reports, especially those being presented to the board of directors or key stakeholders, should include a cover letter commending the participation in a review of business practices. Summarise the steps taken and provide direct contact details to keep the relationship open to discussion and development.

Background

A background is important to set the context of the report. Understanding what the review was benchmarked against and any considerations that were made can assist the vendor with prioritising certain risks and road mapping the response to the report.

Overall Score




Provide an overall score for the third party to easily quantify performance.



Scoring is best when presented in comparison to something useful such as an industry average or in comparison to the performance of a particular cohort or group of vendors utilised by your organisation. Scoring can be as simple or as detailed as necessary depending on the audience receiving the report. For instance, specific scoring in different categories can be provided for IT staff.

Risks/Observations

Be selective in how your organisation refers to the gaps or findings. Some vendors may take the use of “observations” more positively than a term such as “flaws” or “vulnerabilities”. If a lot of risks are identified, you may want to focus on higher priority risks. If this is the case, a disclosure should be made so that the vendor knows additional risks exist.

Severity	Risk
 High	<i>No Business Continuity Plan is in place to manage the occurrence of incidents or disruptions.</i>
 High	<i>No information security or cyber risk awareness training program for all staff.</i>
 Medium	<i>Police/Criminal Record Checks not performed for all staff with access to Information Technology.</i>

Risks can also be presented in a more granular manner by addressing key areas such as Business Continuity, Information Security, People and Staffing, Compliance, Audit and Review, etc.

Recommendations

Merely providing observations can be a great start, but without recommendations to aid the third party, there is not a lot of value added. By providing recommendations for each observation, the commitment to collectively improving business processes will be appreciated. Buying organisations and the third party are part of the same industry and any steps towards better practice by either side is a benefit to the entire sector.

Next Steps

The next steps can help the development of the relationship with a third party. By providing the third party with simple to understand first steps, they can begin or continue their risk journey with confidence. This also gives the buying organisation the opportunity to prioritise what is considered critical remediations for them.

Summary

Like the cover letter, the summary should be used to thank the third party for taking the time to participate in the review. Provide a succinct statement of their overall performance and what impression this has left with the buying organisation. For poor performance, do not be afraid to call out an expectation that prompt action is taken. Equally, do not hesitate to congratulate a good effort, especially if improvements are seen throughout ongoing reviews.

Appendix 2 – Third-Party Review Checklist

Provides guidance on the areas to monitor regularly and at contract renewal.

Does the third party maintain policies and procedures that align with your organisation's ethics and culture?	<input type="checkbox"/>
Has the third-party shown continual improvement of business frameworks to ensure compliance with evolving standards and regulatory requirements?	<input type="checkbox"/>
Has the third-party performance met the requirements of the organisation?	<input type="checkbox"/>
Has service or product quality fallen within the x% agreed/allowed tolerance?	<input type="checkbox"/>
Has the delivery of the vendor met time expectations with minimal changes to scheduling or interruptions?	<input type="checkbox"/>
Does the pricing and fee structure have an appropriately increasing frequency?	<input type="checkbox"/>
Is the vendor proactive about improving processes and increasing efficiency?	<input type="checkbox"/>
Does the vendor comply with the state regulatory requirements within which it resides?	<input type="checkbox"/>
Does the vendor pose any financial viability risk?	<input type="checkbox"/>
Has the vendor identified its key dependencies (fourth and fifth parties)?	<input type="checkbox"/>
Does the vendor have contingency plans for key dependency failures?	<input type="checkbox"/>
Does the vendor maintain ongoing internal audits and independent reviews of processes?	<input type="checkbox"/>
Does the vendor utilise streamlined communication processes, and communicate clearly?	<input type="checkbox"/>
Does the vendor resolve any issues or concerns within an appropriate timeframe?	<input type="checkbox"/>
Does the vendor provide adequate support to both the organisation and end-users?	<input type="checkbox"/>

Appendix 3 – Express Cyber Risk Questionnaire

Provides guidance on the questionnaire to send third parties holding sensitive data.

Do you have an up-to-date information security framework in place?
Are all your cyber risks assessed and catalogued as part of a framework?
Do you allow your employees to access work-related systems on their personal devices (including mobile devices)?
Is your email protected by email domain security policies and anti-spam?
Is multi-factor authentication used by your organisation?
How regularly are security patches applied to your systems (including desktops)?
Does your IT infrastructure adopt better practice security requirements?
Is there a backup and recovery procedure in place to manage incidents?
Do you have a Disaster Recovery or Cyber Incident Plan in place?
Are plans and sub-plans exercised and reviewed as part of a multi-year program?
Do all your staff undergo ongoing cyber risk awareness training?
Are high risk staff vetted and security checks performed during onboarding?
Does physical security and workplace cyber hygiene meet better practice standards?
Have you experienced any cyber-attacks or data breaches in the last 12 months?
Do you have a cyber insurance policy in place?

Appendix 4 – Cyber Security Questionnaire

Provides guidance on the questionnaire to send to IT vendors who provide your business with information technology services.

Do you have an up-to-date information security framework in place that includes a policy, procedures, response plans and clearly defined responsibilities?
Are cyber risks assessed as part of a risk management framework?
Do you have an information asset register in place to identify the location, owner, risks, controls, configuration, processing and recovery of all information stores used?
Are you affected by GDPR or other data protection regulations? Is compliance with regulations documented and reviewed annually?
Is a physical asset register maintained to ensure ongoing maintenance, updating and replacement of devices occurs on schedule?
Do you utilise SPF, DKIM and DMARC policies to protect email and ensure partners are safe from email spoofing?
Do your employees and contractors use multi-factor authentication to access all systems or systems containing organisation data?
Are strict password policies enforced that align with the minimum requirements of the organisation?
Are mobile devices and remote access managed and controlled to enforce acceptable use of technology?
Does application hardening and patching ensure appropriate and protected use?
Has your IT infrastructure been assessed to ensure it employs better practice techniques such as segregation and demilitarised zones?
Is encryption utilised for all data at rest and data in transit? Does the encryption standard align with the minimum requirement of the organisation?
Do any other external entities interact with the data accessed, stored and processed by the organisation?
Are multiple copies/multi-location backups kept ensuring recovery of data and preventing infection or corruption of data?

Is recovery of data tested at least annually as part of a back and recovery program?
Do you have a Disaster Recovery or Cyber Incident Plan in place that is exercised and regularly reviewed?
Is your information security framework reviewed by an independent security consultant to ensure there are sufficient components and measures in place?
Can you provide ISO or SOC report certifications to present compliance, or present the certifications of vendors when services are outsourced?
Do your staff and contractors undergo ongoing cyber risk awareness training and phishing campaigns?
Are police checks performed on all staff and contractors with access to data/information technology?
Is logging and assessments of logs performed on all devices, infrastructure and data transactions?
For any applications, software or logical coding developed in-house, is there a software development lifecycle to manage the process and is secure development managed?
Is there a security program, including physical security, to accompany the information security framework?
Does physical security align with the minimum/better practice requirements? (e.g. swipe cards, clean desk policy, perimeter fencing, CCTV, etc).
Have you experienced any cyber-attacks or data breaches in the last 12 months?
Do you have a process in place for reporting any breaches or after identifying any potential vulnerabilities?
Is there a direct contact within for any security concerns?

References

ISO 37500

Guidance on outsourcing

ISO 44001:2017

Collaborative business relationship management systems

The Institute of Internal Auditors

Auditing Third-Party Risk Management

Ponemon-IBM Security

Cost of a Data Breach Study, years 2017 to 2021

Kaspersky Lab

The State of Industrial Cybersecurity in the Era of Digitalization, September 2020

Australian Prudential Regulation Authority (APRA)

Prudential Standard CPS 231 Outsourcing (no. 6 of 2016), July 2017

Prudential Practice Guide PPG 231 Outsourcing, October 2006

NSW Government

Local Government Act (no. 30 of 1993), October 2020

Forbes

The Rise of Third-Party Digital Risk, July 2020

Gate Keeper

How to Track the Performance of your Key Vendors, April 2018

Monash University

Information Sharing in Supply Chains: A Literature Review and Research Agenda

Contact Us

a Level 35, One International Towers
Barangaroo Sydney Australia

t +61 2 9241 1344

e info@iconsult.com.au

w www.iconsult.com.au



Copyright © 2022 InConsult Pty Ltd. All rights reserved.

This report may not be sold, reproduced or redistributed, in whole or in part, without the prior written permission of InConsult. This report and any recommendations, analysis or advice provided herein (i) are based on our experience as consultants, (ii) are not intended to be taken as advice or recommendations regarding any individual situation, and (iii) should not be relied upon as professional advice regarding any individual situation or as a substitute for consultation with professional consultants or advisors. The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. We are not responsible for the consequences of any unauthorized use of this report. Its content may not be modified or incorporated into or used in other material, or sold or otherwise provided, in whole or in part, to any other person or entity. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Information furnished by others, as well as public information and industry and statistical data, upon which all or portions of this report may be based, are believed to be reliable but have not been verified. Any modelling, analytics or projections are subject to inherent uncertainty, and any opinions, recommendations, analysis or advice provided herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. We have used what we believe are reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied, and we disclaim any responsibility for such information or analysis or to update the information or analysis in this report. We accept no liability for any loss arising from any action taken or refrained from, or any decision made, as a result of or reliance upon anything contained in this report or any reports or sources of information referred to herein, or for actual results or future events or any damages of any kind, including without limitation direct, indirect, consequential, exemplary, special or other damages, even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. No responsibility is taken for changes in market conditions or laws or regulations which occur after the date hereof.