

Internal and Confidential

Netradyne Third Party Risk Management Process & Procedure

v1.1

Table of Contents

[Netradyne Third Party Risk Management Process & Procedure 0](#_Toc166092997)

[Document Control 2](#_Toc166092998)

[1 Purpose 3](#_Toc166092999)

[2 Scope 3](#_Toc166093000)

[3 Roles and Responsibilities 3](#_Toc166093001)

[4 Procedure 4](#_Toc166093002)

[4.1 Third parties can include: 4](#_Toc166093003)

[4.2 Potential Risk Involved with Third-Party: 4](#_Toc166093004)

[4.3 Purpose of TPRM: 5](#_Toc166093005)

[4.4 Benefit of TPRM: 6](#_Toc166093006)

[4.5 Outcome of TPRM: 6](#_Toc166093007)

[4.6 Third Party Engagement Classification 6](#_Toc166093008)

[4.6.1 Negligible Level Engagements: 6](#_Toc166093009)

[4.6.2 Low-Risk Engagements: 6](#_Toc166093010)

[4.6.3 Moderate-Risk Engagements: 6](#_Toc166093011)

[4.6.4 Significant/High-Risk Engagements: 7](#_Toc166093012)

[4.6.5 Critical-Risk Engagements: 7](#_Toc166093013)

[4.7 Third-Party Risk Management Workflow: 7](#_Toc166093014)

[4.7.1 Sourcing & Screening of Third-Party 7](#_Toc166093015)

[4.7.2 Due Diligence: 9](#_Toc166093016)

[4.7.3 Listing, Evaluation and Risk Categorization of Third-Party : 9](#_Toc166093017)

[4.7.4 Risk Assessment & Recommendations: 9](#_Toc166093018)

[4.7.5 Decision Making, Draft & Finalize Contractual Protections: 12](#_Toc166093019)

[4.7.6 Ongoing Monitoring: 12](#_Toc166093020)

[4.7.7 Incident Response and Remediation for Third Party specific engagements: 12](#_Toc166093021)

[4.7.8 Continuous Improvement: 13](#_Toc166093022)

[4.8 RACI Matrix for Third Party Life Cycle Management 14](#_Toc166093023)

[5 Conduct 15](#_Toc166093024)

[6 Exception 15](#_Toc166093025)

[7 Terms/Acronyms 15](#_Toc166093026)

[8 References 15](#_Toc166093027)

[8.1 Templates 15](#_Toc166093028)

[8.2 Policies 15](#_Toc166093029)

[8.3 Process/Procedures 15](#_Toc166093030)

[8.4 Standards 15](#_Toc166093031)

[8.5 Miscellaneous 15](#_Toc166093032)

[9 Appendix A: Document RACI Matrix 16](#_Toc166093033)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDTPRM2024001 |
| **Document Name** | Netradyne InfoSec Third Party Risk Management Process & Procedure |
| **Document Status** | Draft |
| **Document Released Date** | 10-MAY-2024 |
| **Document Author** | Sudhansu Kumar |
| **Document Content Contributors** | Sudhansu Kumar |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Saravanan Sankaran |
| **Document Version** | v1.1 |
| **Information Classification** | Internal & Confidential |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 10-MAY-2024 | Original issue | Sudhansu Kumar |
| V1.1 | 31-JAN-2025 | Reviewed with no changes | Kavitha Shetty |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 10-MAY-2024 | Saravanan Sankaran | Senior Director InfoSec & IT | Approved |
| 04-FEB-2025 | Saravanan Sankaran | Senior Director InfoSec & IT | Approved |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| All Employees | Netradyne |
|  |  |
|  |  |

# Purpose

Third party service providers (TPSP) offer a necessary adjunct to NETRADYNE’s capabilities. By providing services or specialized support utilizing contract resources over short periods of time, NETRADYNE can achieve both operating and financial efficiencies that would otherwise require long term commitments or capital investments.

Relationships with outside service personnel and organizations, however, present unique legal and operational situations that are addressed cautiously in order to successfully fulfil NETRADYNE’s objectives. Because of the sensitive nature of NETRADYNE operations and the data it processes, security is a foremost consideration in the establishment and maintenance of these relationships.

It is the intent of the policies in this section to ensure that outside Information Technology services provided to the NETRADYNE do not jeopardize the integrity of the NETRADYNE’s security program.

# Scope

The provisions outlined in this document are applicable to the operations and activities on behalf of NETRADYNE of both service organizations and contract personnel, regardless of whether the service is provided on or off NETRADYNE premises.

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# Procedure

A "Third Party" refers to any external entity that is involved in a business transaction or relationship but is not directly part of the Netradyne.

## Third parties can include:

* Vendors
* Suppliers
* Contractors
* Service Providers
* Consultants
* Business Partners
* Outsourcing Companies
* And Other External Entities.

Third-party risk management (here onwards will be called “TPRM”) is the process of identifying, assessing, and mitigating the risks associated with engaging third-party vendors or partners. It involves evaluating the potential impact that third-party relationships can have on Netradyne's operations, reputation, financial stability, regulatory compliance, and overall security posture.

## Potential Risk Involved with Third-Party:

* **Reputation Risk:** The damage that can occur to a business when it fails to meet the expectations of its stakeholders and is thus negatively perceived with customers
* **Strategic Risk:** The risks of failing to achieve the business objectives and outcomes
* **Data Privacy Risk**: The potential loss of control over any personal/sensitive information during the engagement
* **Financial Risk:** The threat that hampers financial growth and company's profitability
* **Regulatory Risk:** Leading to non-compliance to meet laws, regulatory expectations
* Operational risk: The risk of losses caused by flawed or failed processes, policies, systems or events that disrupt business operations and resiliency
* **Technology Risk:** Any potential for technology failures to disrupt our business such as information security incidents, service outages, stability and availability

## Purpose of TPRM:

* To assess third-party vendor risks which potentially exposes Netradyne to any kind of attacks, data breaches, and reputational damage.
* This is particularly important for high-risk vendors who process Personal identifiable Information (PII)/Protected Health Information (PHI)/ Netradyne Sensitive Information (SI) / Customer data, or Netradyne Intellectual property
* As vendors have access to our PII/sensitive data, it's our responsibility to safeguard our data

## Benefit of TPRM:

* This can support us proactively to assess the risk before arriving the decision of engaging vendors and monitoring
* To identify any issues that warrant a restructuring of the deal
* Ability to surface third-party risks before it’s too late to remediate
* Allow for the identification and quantification of a vendor’s Infosec posture

## Outcome of TPRM:

* This will mature in safeguarding Netradyne environment from all types of risk
* This will enable Netradyne to meet regulatory requirement as data controller and data processor
* Understand the threat landscape and identify common threats

## Third Party Engagement Classification

Third-party engagement classification levels refer to the categorization of third-party relationships by Netradyne based on factors such as:

* The Level Of Risk,
* Importance To The Organization,
* And The Nature Of Services Provided.

These classification levels help Netradyne to prioritize its Third-Party Risk Management efforts and allocate resources accordingly. Netradyne InfoSec defines a general framework for classifying third-party engagements into different levels:

### Negligible Level Engagements:

* These are third-party relationships with negligible risk exposure to Netradyne. This Third Party may have ad hoc/one time partnership with Netradyne.
* They don't capture any Netradyne data. Their security posture is not so important for Netradyne engagement.
* **Signed Non-Disclosure Agreement (NDA)** is sufficient for such engagements.

### Low-Risk Engagements:

* These are third-party relationships with minimal risk exposure to Netradyne.
* Examples may include non-critical vendors providing low-value goods or services that do not involve access to sensitive data or critical systems.
* Low-risk engagements may require minimal oversight and monitoring, with standard contractual agreements and basic due diligence checks.
* Many a time **Signed Non-Disclosure Agreement (NDA)** is sufficient for such engagements.
* Netradyne may or may not uses [TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP) (depends on assessor discretion) to assess the security and maturity level of such Third-Parties.

### Moderate-Risk Engagements:

* Moderate-risk engagements involve third-party relationships that have some level of risk exposure to the organization but are not deemed critical or high-risk. They hardly capture any Netradyne data (sensitive/confidential). Examples may include vendors providing essential services or products that are not directly related to core business operations.
* Moderate-risk engagements may require more comprehensive due diligence, risk assessment, and contractual protections compared to low-risk engagements. Ongoing monitoring and periodic reviews are also recommended.
* Netradyne uses [TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP) to assess the security and maturity level of such Third-Parties.

### Significant/High-Risk Engagements:

* Significant or High-risk engagements involve third-party relationships that pose significant risk exposure to the organization due to factors such as the criticality of services provided, access to sensitive data or systems, or regulatory compliance requirements.
* Examples may include key suppliers, strategic partners, service providers with access to confidential information, or vendors involved in critical business processes.
* Significant or High-risk engagements typically require thorough due diligence, comprehensive risk assessment, detailed contractual agreements with robust security and compliance requirements, and ongoing monitoring and oversight. Regular audits and assessments may also be necessary to ensure compliance and mitigate risks effectively.
* Netradyne leverage [TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP) to assess the security and maturity level of such Third-Parties.

### Critical-Risk Engagements:

* Critical-risk engagements represent third-party relationships that are mission-critical or essential to the Netradyne's core business operations, continuity, and success.
* Examples may include outsourcing partners, cloud service providers hosting critical systems or data, or vendors with access to highly sensitive information.
* Critical-risk engagements demand the highest level of scrutiny, oversight, and risk management controls. They require extensive due diligence, rigorous risk assessment, stringent contractual agreements with detailed security and compliance requirements, and continuous monitoring and evaluation to mitigate risks effectively and ensure business resilience.
* Netradyne uses Netradyne [TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP) as **Stage 1** to assess the security and maturity level of such Third-Parties as an initial assessment.
* Afterwards Netradyne performs an [InfoSec Detailed Risk Assessment](https://netorg726775.sharepoint.com/:f:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/InfoSec%20Detailed%20TPRM%20Assessment?csf=1&web=1&e=ZjQGxn) as **Stage 2** for its critical vendor at periodic basis.

By classifying third-party engagements into different risk levels, Netradyne can prioritize their efforts and resources to focus on managing risks effectively based on the criticality and importance of each relationship. This approach helps Netradyne to allocate resources efficiently, enhance their risk management capabilities, and safeguard their assets, reputation, and business continuity.

## Third-Party Risk Management Workflow:

### Sourcing & Screening of Third-Party

Sourcing & Screening of third party refers to the activities involved in identifying, evaluating, and selecting external vendors or partners to fulfil Netradyne specific business needs or requirements. It's a crucial stage in the third-party onboarding process, as it lays the foundation for establishing successful and mutually beneficial relationships with external entities.

* For smaller or urgent engagements, Netradyne has the liberty to by-pass these systematic procedures.
* Third Party Risk Management Process and Evaluation may go in parallel with this stage.

Here's various stages of the sourcing & Screening process in third-party onboarding:

#### Identifying Business Needs:

The sourcing process begins with identifying the specific business needs, objectives, or requirements that necessitate engaging external vendors or partners. This involves conducting a thorough analysis of the Netradyne's strategic goals, operational gaps, resource constraints, and project requirements.

#### Market Research:

Once the business needs are identified, Netradyne conduct market research to identify potential vendors or partners that can meet those needs. This may involve researching industry directories, attending trade shows, soliciting referrals, leveraging professional networks, and conducting online searches to compile a list of potential candidates.

#### Vendor Evaluation:

Netradyne shall evaluate potential vendors or partners based on various criteria, such as their capabilities, expertise, experience, reputation, financial stability, geographic location, compliance with regulatory requirements, and alignment with Netradyne’s values and objectives. This evaluation process may include reviewing vendor qualifications, conducting background checks, requesting references, and assessing vendor performance through interviews, demonstrations, or site visits.

#### Request for Proposal (RFP) or Request for Quote (RFQ):

Once a shortlist of potential vendors is identified, organizations may issue a formal Request for Proposal (RFP) or Request for Quote (RFQ) to solicit detailed information and pricing proposals from vendors. The RFP or RFQ typically outlines the project scope, requirements, evaluation criteria, timeline, and submission instructions.

#### Vendor Selection:

After receiving and evaluating vendor proposals, Netradyne select the most suitable vendor(s) based on factors such as cost-effectiveness, technical capabilities, quality of service, responsiveness, scalability, and compatibility with Netradyne’s needs and objectives. This selection process may involve cross-functional teams, stakeholder input, and decision-making criteria established during the evaluation phase.

#### Negotiation and Contracting:

Once a vendor is selected, Netradyne negotiate the terms and conditions of the contract, including pricing, payment terms, service-level agreements (SLAs), deliverables, milestones, intellectual property rights, confidentiality provisions, dispute resolution mechanisms, and termination clauses. The goal is to reach a mutually acceptable agreement that addresses the needs and interests of both parties while mitigating risks and ensuring compliance with regulatory requirements.

#### Onboarding and Integration:

After finalizing the contract and TPRM clearance, Netradyne initiate the onboarding and integration process to seamlessly integrate the selected vendor into their operations, systems, and processes. This may involve providing access to relevant resources, conducting orientation sessions, establishing communication channels, defining roles and responsibilities, and setting performance expectations to ensure a smooth transition and alignment with organizational goals.

#### Ongoing Vendor Management:

Once the vendor is onboarded, Netradyne continue to manage and monitor the vendor relationship throughout the contract lifecycle. This includes establishing governance structures, conducting regular performance reviews, addressing issues or concerns in a timely manner, fostering open communication, and collaborating with vendors to drive continuous improvement and value realization.

By following these steps, Netradyne can effectively navigate the sourcing process in third-party onboarding to identify, evaluate, and select the right vendors or partners to support their business objectives and drive success.

### Due Diligence:

Netradyne conducts due diligence on third-party vendors and partners to verify their credentials, reputation, regulatory compliance, maturity, security controls, and adherence to industry standards and best practices. Review contracts, service level agreements (SLAs), security certification reports, Trust Centres, and other legal/InfoSec artifacts to ensure that they adequately address Security And Risk Management requirements.

### Listing, Evaluation and Risk Categorization of Third-Party :

Identify and catalogue all third-party relationships within Netradyne, including the nature and scope of their involvement, the services provided, and the data or systems accessed. Assess the potential risks associated with each third-party relationship, including operational, financial, reputational, compliance, and cybersecurity risks.

Maintain a comprehensive Third-Party listing with their Engagement classifications, the services provided, and the data or systems accessed, Security & Maturity level, Internal & External Stakeholders Names, Date of Review Initiation & Closure, Review Status, Recommendations if any etc.

### Risk Assessment & Recommendations:

Evaluate the inherent information security risks posed by third-party relationships based on factors such as:

* The criticality of the services provided,
* The sensitivity of the data involved,
* The geographic location of the third party,
* Their past reputation and stability,
* and their security controls and practices.

Netradyne InfoSec uses TPRM Risk Assessment Questionnaires, detailed audits, interviews, and other assessment methods to determine the level of risk posed by each third party depending on their level of engagement with Netradyne.

[InfoSec TPRM Review](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=pgILyD) is applicable if any of the below condition satisfies:

1. Netradyne data (or Netradyne’s client data) except the publicly available data, is hosted/Stored/Accessed/Processed by Third Party.
2. Netradyne system(s) is accessed/connected/integrated to Third Party System(s)/App/APIs/Person.
3. Third party will provide critical service/function to Netradyne and any disruption arises from Third Party side, may lead to service outage to Netradyne or Netradyne’s client.

Please determine which condition(s) are getting satisfied. If none are applicable, infosec review is not required and signing the Non-Disclosure Agreement (NDA) will suffice the requirements. For NDA, @Netradyne Legal Team can support.

If any of these conditions are satisfied, Netradyne InfoSec need to follow the following type of Risk Assessment, as per [Third Party Engagement Classification](#_Third_Party_Engagement):

|  |  |  |
| --- | --- | --- |
| **#** | **Third Party Engagement Classification** | **Type of TPRM Risk Assessment Performed** |
| 1 | Critical-Risk Engagements | * Netradyne uses Netradyne [TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP) as **Stage 1** to assess the security and maturity level of such Third-Parties as an initial assessment. * Afterwards Netradyne performs an [InfoSec Detailed Risk Assessment](https://netorg726775.sharepoint.com/:f:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/InfoSec%20Detailed%20TPRM%20Assessment?csf=1&web=1&e=ZjQGxn) as **Stage 2** for its critical vendor at periodic basis. |
| 2 | Significant/High-Risk Engagements | * Netradyne leverage [TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP) to assess the security and maturity level of such Third-Parties with focus monitoring of contracts, changes and incident management measures. |
| 3 | Moderate-Risk Engagements: | * Netradyne uses [TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP) to assess the security and maturity level of such Third-Parties. |
| 4 | Low-Risk Engagements | * Many a time **Signed Non-Disclosure Agreement (NDA)** is sufficient for such engagements. * Netradyne may or may not uses [TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP) (depends on assessor discretion) to assess the security and maturity level of such Third-Parties. |
| 5 | Negligible Level Engagements | * **Signed Non-Disclosure Agreement (NDA)** is sufficient for such engagements. |

**How to initiate a TPRM Assessment Request:**

**Requester(s) or TPRM co-ordinator(s) are supposed to follow the procedure to initiate the TPRM assessment using** [**Netradyne TPRM Assessment Work-Flow**](https://netorg726775.sharepoint.com/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/General/TPRM/TPRM%20Artifacts%20to%20Share%20with%20Third%20Parties/Netradyne_TPRM_AssessmentWorkflow.docx?web=1)**.**

[InfoSec TPRM Review](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=pgILyD) is applicable if any of the below condition satisfies:

1. Netradyne data (or Netradyne’s client data) except the publicly available data, is hosted/Stored/Accessed/Processed by Third Party.
2. Netradyne system(s) is accessed/connected/integrated to Third Party System(s)/App/APIs/Person.
3. Third party will provide critical service/function to Netradyne, and any disruption arises from Third Party side, may lead to service outage to Netradyne or Netradyne’s client.

Please determine which condition(s) are getting satisfied. If none are applicable, infosec review is not required and signing the NDA will suffice the due diligence. For NDA, @Legal can help you.

If any condition(s) satisfies, Please:

* Open a Service Desk Ticket using [SD+ -> InfoSec Services -> TPRM Assessment Request Template](https://itservicedesk.netradyne.com/app/itdesk/ui/requests/add?reqTemplate=155142000001496140) ([click the link](https://itservicedesk.netradyne.com/app/itdesk/ui/requests/add?reqTemplate=155142000001496140)) for TPRM workflow, records and approvals.
* Get the NDA signed with the vendor. That is the preliminary condition before sharing our TPRM review Questionnaire with them.
* Open the [TPRM questionnaire spreadsheet](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=pgILyD) and do the following:
  + Provide the third-party (vendor/supplier etc.) name. (See Step 2)
  + Provide the engagement specific information at the designated place on the cover page (See Step 2)
* Share the questionnaire with the Vendor and ask them to provide the response and below mentioned artifacts.

Artifacts Requirements for InfoSec TPRM review closure:

* Filled TPRM questionnaire
* Copy of Security certification from Vendor if they have any (E.g., ISO 27001, SOC 2 etc.)
* Latest VAPT report/summary report for their Infrastructure/software/APIs, if getting used in this engagement.

This is a preliminary security check, having minimal nos. of queries (21 in total). Vendor can provide their responses using drop downs. If anything, additional they want to convey, they may use the comment section. For detailed instructions responder may see the “Support for Response” tab, that’s step-by-step guidance to fill up the responses. Ideally, It should not take more time as only twenty-one checks need to be responded.

For any such TPRM Review request initiation the TPRM CO-ORDINATOR (e.g. Netradyne Personnel responsible for initiating the TPRM request and/or managing Third-Party Onboarding) can contact [TPRM@Netradyne.com](mailto:TPRM@Netradyne.com) & [InfoSec@Netradyne.com](mailto:InfoSec@Netradyne.com).

**This will enable the quick and effective turnaround to:**

Before sharing the TPRM Assessment Spreadsheet with the responder, TPRM Co-Ordinator has to perform the following changes:

STEP 1: Download a copy of original TPRM Assessment Accelerator from the below link:

[Netradyne TPRM Assessment Accelerator.xlsx](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=ktJagI)

STEP 2: Provide the Vendor/Third Party name to one specific Cell:

A screenshot of a computer

Description automatically generated

2. Provide the name of the Third Party/Vendor

1. Open this tab and provide the vendor/third-party name in the above pink coloured cell.

You also need to provide the engagement specific information at TPRM Review Questionnaire->CoverPage as shown below:

|  |  |
| --- | --- |
| **Please Provide Below Information (Responder Responsibility)** | |
| Netradyne Sponsor: |  |
| Netradyne Program Manager: |  |
| Name of the Organization: |  |
| Purpose of engagement: |  |
| Period of engagement: |  |
| Name of the Respondent(For this checklist): |  |
| Contact Information(Email ID, Organization address, and office contacts) |  |

STEP 3: Share the TPRM Questionnaire to requesting stakeholder to fill the responses and send back.

For any query/ambiguity, feel free to contact [Netradyne InfoSec team](mailto:Infosec@netradyne.com?subject=TPRM%20INITIATION/QUERY).

### Decision Making, Draft & Finalize Contractual Protections:

Once InfoSec, Privacy, IT, HR & Finance, and other associated stakeholders (If any) has provided their clearance to go ahead with the proposed engagement, Legal Team in consultation with the Requester has to establish contractual protections and provisions in Master Service Agreement (MSA) to mitigate third-party risks. Legal has to vet and finalize the MSA.

**This may include:**

* Indemnification Clauses,
* Liability Limitations,
* Data Protection Requirements,
* Confidentiality/Privacy Obligations,
* Security Standards,
* Audit Rights,
* Recommendations stemming from TPRM Assessments
* And Breach Notification Procedures.

Ensure that contracts clearly define each party's responsibilities, obligations, and liabilities related to risk management.

### Ongoing Monitoring:

Netradyne implements procedures and controls for ongoing monitoring of **Important/Critical Third-Party Relationships** to detect changes in risk exposure, performance issues, compliance violations, security incidents, or other developments that may impact the organization. Periodic reviews, assessments, audits, and security assessments of third-party vendors are conducted to ensure continued compliance with contractual obligations and security standards.

### Incident Response and Remediation for Third Party specific engagements:

Netradyne has identified incident response and remediation plans to address security breaches, data breaches, service disruptions, or other incidents involving third-party vendors. Netradyne establishes communication channels, escalation procedures, and coordination mechanisms to facilitate rapid response and recovery efforts in collaboration with third-party partners.

### Continuous Improvement:

Netradyne continuously evaluate and improve the org wide third-party risk management program based on lessons learned, feedback, industry trends, regulatory changes, emerging threats, and evolving business needs. It incorporate feedback from stakeholders, internal audits, and external assessments to enhance the effectiveness and maturity of the TPRM program over time.

By effectively managing third-party risks, Netradyne can strengthen its resilience, protect its assets and reputation, ensure regulatory compliance, and maintain trust and confidence with customers, partners, and stakeholders. Third-party risk management is an essential component of overall risk management and cybersecurity strategy at Netradyne's interconnected and complex business environment.

## RACI Matrix for Third Party Life Cycle Management

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Activity | Duration (Max.) | Third Party | Requester/TPRM Co-Ordinator | Finance | Legal | Privacy | IT | HR | InfoSec | ND Leadership |
| Sourcing & Screening | Initial Process  (May run in parallel with TPRM Review) | R | R,A | I | - | - | - | - | - | - |
| Due Diligence | 3 Days | R | R,A | I | R | R | I | I | R | - |
| Listing, Evaluation and Risk Categorization | Ongoing | - | R | R | R | R | R | R | R,A | - |
| Risk Assessment & Recommendations | (7+3) Days | R | R | - | R,A  (Legal Risk) | R,A  (Privacy Risk) | C | C | R,A  (InfoSec Risk) | I |
| Decision Making, Finalization & Onboarding | 5 Days | R | R | R | R | C | R | R | C | R,A |
| Ongoing Monitoring | Ongoing | R | R,A | - | C | C | C | C | R | - |
| Incident Response and Remediation | Ongoing | R | R,A | - | C | C | C | C | C | - |
| Continuous Improvement | Ongoing | R | R,A | C | R | R | R | R | R | C |
| Termination & Offboarding | 5 Days | R | R,A | R | R | C | R | R | C | C |

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

Exception to this procedure must be approved through the Netradyne Exception Process.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| TPRM | Third Party Risk Management |
| PII | Personal Identifiable Information |
| PHI | Protected Health Information |
| ND | Netradyne |
|  |  |
|  |  |
|  |  |

# References

## Templates

<List of (or Links to) associated templates>

## Policies

[Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=mRSIq4)

[Netradyne Information Security Exception Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Exception%20Process.pdf?csf=1&web=1&e=RbfEhO)

[Acceptable Usage Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Acceptable%20Usage%20Policy.pdf?csf=1&web=1&e=2jMnrk)

## Process/Procedures

[NETRADYNE DISASTER RECOVERY PROCESS.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20DISASTER%20RECOVERY%20PROCESS.pdf?csf=1&web=1&e=xTyHtp)

[NETRADYNE BUSINESS CONTINUITY PLAN.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20BUSINESS%20CONTINUITY%20PLAN.pdf?csf=1&web=1&e=eCZUy6)

[Netradyne Vulnerability & Patch Management Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Vulnerability%20%26%20Patch%20Management%20Process.pdf?csf=1&web=1&e=N697w0)

[NetradyneSecurityIncidentResponsePlan.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NetradyneSecurityIncidentResponsePlan.pdf?csf=1&web=1&e=Nzo34K)

[Netradyne TPRM Assessment Work-Flow](https://netorg726775.sharepoint.com/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/General/TPRM/TPRM%20Artifacts%20to%20Share%20with%20Third%20Parties/Netradyne_TPRM_AssessmentWorkflow.docx?web=1)

## Standards

<List of (or Links to) related Netradyne Standards>

## Miscellaneous

[TPRM Assessment Accelerator](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Assessment%20Accelerator.xlsx?d=wfa4cab9cfed14aae832fec560604e051&csf=1&web=1&e=5PifhP)

[InfoSec Detailed Risk Assessment](https://netorg726775.sharepoint.com/:f:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/InfoSec%20Detailed%20TPRM%20Assessment?csf=1&web=1&e=ZjQGxn)

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Role/Activity | Document Owner/Functional Area Lead | Document Contributor | ND Leadership | Functional Area Team | InfoSec | All ND Member(s) |
| Ensure document is kept current | A | R | I, C | R, C | C | I |
| Ensure stakeholders are kept informed | A | R | - | R | C | - |
| Ensure document contains all relevant information | A | R | I, C | R, C | C | I |
| Ensure document adheres to document governance policy | A, R | R | I | R, C | R, C | I |
| Provide SME advice | I, R | A, R | I | R, C | I, C | I |
| Gathering and adding document contents | I | A, R | I, C | R, C | C | I |
| Document Approval | A | R | I, R | I | I, R | I |

|  |  |
| --- | --- |
| Key |  |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |