End-to-End Third-Party Risk Due Diligence & Issue Management

ServiceNow TPRM | Mock Vendor: Mimickme Ltd.

Overview

This project demonstrates an end-to-end Third-Party Risk Management (TPRM) lifecycle implemented in ServiceNow, covering intake, onboarding, inherent risk assessment, risk-based external due diligence, issue management, and formal risk closure.

The workflow was executed in a controlled ServiceNow training environment using a mock vendor and engagement to reflect real-world regulatory and enterprise TPRM expectations.

Business Objective

Enable risk-based onboarding of a third party responsible for processing credit card information, ensuring that:

- Due diligence is completed **before engagement approval**
- Risk scoping is **proportional to inherent risk**
- Control gaps are **identified, tracked, and remediated**
- All decisions are **auditable and defensible**

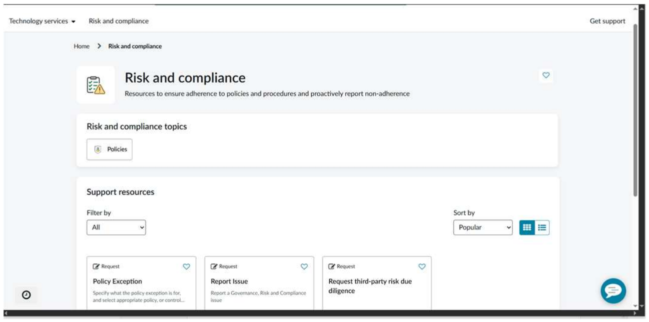
This approach reflects how mature organizations operationalize third-party risk rather than relying on ad hoc questionnaires or manual reviews.

Scope of Work

- Third-party onboarding and engagement creation
- Inherent risk questionnaire (IRQ) and tiering
- Risk-based triggering of external assessments
- Third-party collaboration via secure portal
- Issue identification, escalation, remediation, and closure
- Final risk rating and engagement readiness

TPRM Lifecycle Implemented

1. **Request Due Diligence (Governed Intake)**
   A formal due diligence request was initiated through the ServiceNow Employee Center, ensuring that third-party onboarding could not proceed without risk review and accountability.



Risk and compliance

Resources to ensure adherence to policies and procedures and proactively report non-adherence

Risk and compliance topics

Support resources

Filter by: All

Sort by: Popular

Policy Exception

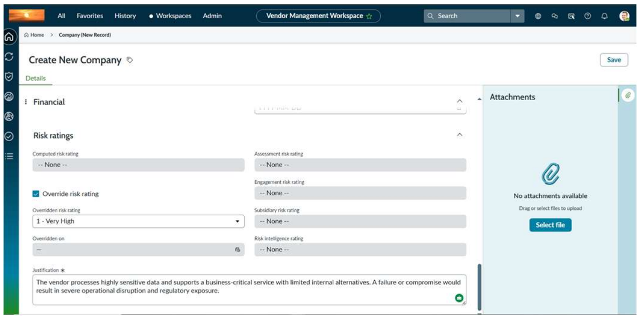
Specify what the policy exception is for, and select appropriate policy, or control...

Report Issue

Report a Governance, Risk and Compliance issue

Request third-party risk due diligence

2. **Third-Party & Engagement Onboarding**
   The third party and engagement were created and scoped within a managed onboarding workflow under third-party risk management oversight.
3. **Inherent Risk & Tiering (IRQ)**
   An inherent risk questionnaire was completed to assess:
   - Sensitive data access
   - Regulatory exposure
   - Operational dependency



Create New Company

Risk ratings

Computed risk rating: -- None --

Assessment risk rating: -- None --

Engagement risk rating: -- None --

☑ Override risk rating

Overridden risk rating: 1 - Very High

Subsidiary risk rating: -- None --

Overridden on: --

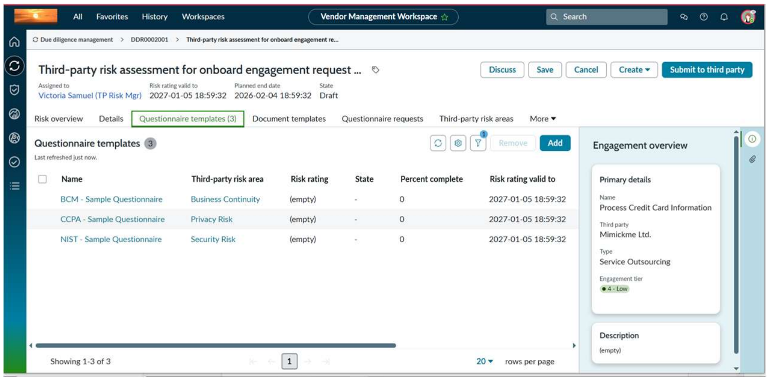
Risk intelligence rating: -- None --

Justification *

The vendor processes highly sensitive data and supports a business-critical service with limited internal alternatives. A failure or compromise would result in severe operational disruption and regulatory exposure.

The results determined the risk tier and drove downstream due diligence requirements.

4. **Risk-Based External Due Diligence**
   External questionnaires (Security, Privacy, Business Continuity) were **system-triggered** based on IRQ responses.
   This ensured proportional due diligence rather than a one-size-fits-all approach.



Due diligence management > DDR0002001 > Third-party risk assessment for onboard engagement re...

Third-party risk assessment for onboard engagement request ...

Assigned to: Victoria Samuel (TP Risk Mgr)
Risk rating valid to: 2027-01-05 18:59:32
Planned end date: 2026-02-04 18:59:32
State: Draft

Questionnaire templates 3
Last refreshed just now.

Name	Third-party risk area	Risk rating	State	Percent complete	Risk rating valid to
BCM - Sample Questionnaire	Business Continuity	(empty)	-	0	2027-01-05 18:59:32
CCPA - Sample Questionnaire	Privacy Risk	(empty)	-	0	2027-01-05 18:59:32
NIST - Sample Questionnaire	Security Risk	(empty)	-	0	2027-01-05 18:59:32

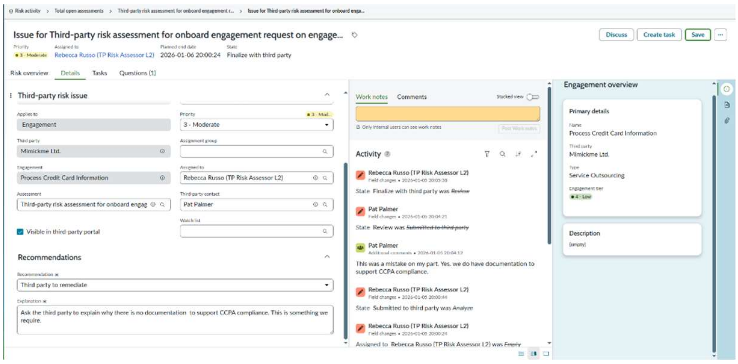
Showing 1-3 of 3 · 1 · 20 rows per page

Engagement overview

Primary details
Name: Process Credit Card Information
Third party: Mimickme Ltd.
Type: Service Outsourcing
Engagement tier: ● 4 - Low

Description
(empty)

5. **Third-Party Assessment Portal Collaboration**
   The vendor responded to assessments through the Third-Party Assessment Portal, improving auditability, reducing email-based risk, and enabling structured collaboration.
6. **Issue Identification & Escalation**
   A privacy-related control gap was identified during assessment review, resulting in:
   - Formal risk issue creation
   - Defined ownership and priority
   - Visibility to the third party
   - Documented rationale and next steps
7. **Issue Resolution & Closure**
   The third party provided clarification and supporting evidence.
   The issue was reviewed, accepted, and formally closed with a complete audit trail.



Risk activity > Total open assessments > Third-party risk assessment for onboard engagement r... > Issue for Third-party risk assessment for onboard enga...

Issue for Third-party risk assessment for onboard engagement request on engage...

Priority: ● 3 - Moderate
Assigned to: Rebecca Russo (TP Risk Assessor L2)
Planned end date: 2026-01-06 20:00:24
State: Finalize with third party

Third-party risk issue
Applies to: Engagement
Priority: 3 - Moderate
Third party: Mimickme Ltd.
Assignment group:
Engagement: Process Credit Card Information
Assigned to: Rebecca Russo (TP Risk Assessor L2)
Assessment: Third-party risk assessment for onboard engag
Third-party contact: Pat Palmer
Watch list:
☑ Visible in third-party portal

Recommendations
Recommendation: Third party to remediate
Explanation: Ask the third party to explain why there is no documentation to support CCPA compliance. This is something we require.

Only internal users can see work notes

Activity

Rebecca Russo (TP Risk Assessor L2)
Field changes • 2026-01-05 20:05:38
State Finalize with third party was ~~Review~~

Pat Palmer
Field changes • 2026-01-05 20:04:21
State Review was ~~Submitted to third party~~

Pat Palmer
Additional comments • 2026-01-05 20:04:12
This was a mistake on my part. Yes. we do have documentation to support CCPA compliance.

Rebecca Russo (TP Risk Assessor L2)
Field changes • 2026-01-05 20:00:44
State Submitted to third party was *Analyze*

Rebecca Russo (TP Risk Assessor L2)
Field changes • 2026-01-05 20:00:24
Assigned to Rebecca Russo (TP Risk Assessor L2) was ~~Empty~~

Engagement overview

Primary details
Name: Process Credit Card Information
Third party: Mimickme Ltd.
Type: Service Outsourcing
Engagement tier: ● 4 - Low

Description
(empty)

8. **Final Risk Rating & Engagement Readiness**
   Final third-party and engagement risk ratings were documented with justification, enabling informed approval and ongoing monitoring aligned to risk.

Framework & Regulatory Mapping

OSFI B-10 (Third-Party Risk Management)

- Pre-engagement due diligence and approval
- Risk-based tiering and proportional controls
- Documented issue remediation and accountability

ISO/IEC 27001

- A.5 – Risk Management
- A.15 – Supplier Relationships
- Evidence-based control assessment

SOC 2 (Trust Services Criteria)

- CC1 – Governance
- CC3 – Risk Assessment
- CC7 – Incident & Issue Management

Key Outcomes

- Demonstrated a **governed, auditable TPRM workflow**
- Applied **risk-based decision-making**, not checkbox compliance
- Translated regulatory expectations into **operational controls**
- Showed how GRC tools enable **scale, consistency, and defensibility**

Tools & Platforms

- ServiceNow Third-Party Risk Management (TPRM)