Maynard Partners LLC

Template: Information Security Policy - Third-Party Risk Management

Table of Contents

1 Policy Statement

1.1 Use of Third-Party Service Providers:

<District Name Here> utilizes third-party service providers, also referred to as suppliers or vendors, collectively "Service Providers," to outsource a number of operational functions and to procure products and services on behalf of the company.

Such third-party relationships provide substantial value to the company, because they are able to support strategic objectives and increase company expertise while maximizing efficiencies and cost savings opportunities.

As company operations expand digitally, it is common for <District Name Here> to share access to data and/or systems with its Service Providers. The sharing of data access creates potential risk for <District Name Here> A data breach or compromise committed by Service Provider could result in substantial harm to consumers, employees, partners and to the company, resulting in high costs, fines, lawsuits, loss of sales and damage to reputation and customer trust.

1.2 Benchmarking on Cost of Data Breach:

In 2018, research was conducted to benchmark the potential costs related to a large-scale data breach at <District Name Here>. Using the 2017 Equifax breach as a baseline for a hypothetical breakdown of potential costs:

- Net expenses for 1 quarter of $69 million (total cost from Equifax was $242 million) – compiled of $46 million for IT and data security; $29 million for legal and investigative fees; $4 million for product liability (includes legal defense costs relating to not building secure systems to a particular standard or mishandling post-breach duties); minus a net benefit of $10 million in insurance payments.
- e-Commerce loss of 50,000 orders (multiplied by average $ order size) – due to a retail business disruption spanning one morning.
- $12 million in government fines – due to non-compliance with data security laws and using the GDPR 4% of global revenue fine as example. As of 2018, regulation on data security is increasing, although regulatory fines remain rare.

Due to the risk posed by Service Provider data breach, all Service Providers utilized by <District Name Here> must have sufficient controls and processes in place to protect corporate, employee, partner, customer and user data which is collected, generated, maintained and entrusted on behalf of <District Name Here>

1.3 Third-Party Risk Management Program Is Required to Ensure Security Controls

A Third-Party Risk Management (TPRM) program is necessary to provide oversight of qualifying Service Providers and to support InfoSec in identifying and appropriately managing and mitigating the risk of harm posed by Service Providers with access to <District Name Here> data and systems. Certain Service Providers carry the potential for greater risk than others due to factors including, industry, company maturity level,

geolocation, financial health, type of data accessed and usage of data. As a result, TPRM must employ a risk-based approach to identify, monitor and mitigate these greater areas of risk.

1.4 Elements of TPRM Program

The TPRM compliance management lifecycle shall include identification of obligations and risk, communication, controls, due diligence and ongoing monitoring, reporting and continuous improvement.

The TPRM Program shall be both proactive and reactive, prescribing sufficient controls to prevent issues and also responding to non-conformities with remediation, as well as identifying and recommending improvements. In addition, TPRM Program shall have access to a central database of third parties and attributes and shall employ a risk stratification plan and risk scoring model to inform auditing cadence.

Regular reporting shall be provided to key stakeholders on TPRM Program performance and quarterly audit results.

2 Program Objectives

The objectives of the TPRM Program and security risk framework are to:

- Demonstrate an effective and operational Service Provider security risk management program to auditors, regulators, and customers;
- Assess the security posture and detect and mitigate potential risk of Service Provider applications and IT services that are being used by the organization, including private, hybrid, and public cloud infrastructures;
- View the dependencies and assess IT security risks across multiple vendors, software, and Service Providers/IT outsourcing relationships across information supply chain;
- Provide mandate-based reporting on Service Provider security compliance requirements;
- Demonstrate to regulators and auditors that Service Providers are managing their own third-party security risks (<District Name Here>'s 4th party, et seq. risks)

3 Scope & Definitions

TPRM includes all third-party service providers and all third-party solutions and products which either process, store, transmit or receive information; and/or which connect to the <District Name Here> Network for the transmission or reception of <District Name Here> data.

3.1 Third-Party Service Providers

Third-Party Service Providers are those with whom <District Name Here> has either a data sharing or outsourcing relationship and is responsible for either: collecting, processing, storing or deleting <District Name

Here> data; and/or collecting, processing, or storing cardholder payments/data on behalf of <District Name Here>; and/or managing <District Name Here>'s critical business processes or services.

3.2 Critical Business Process

A critical business process is one which must be restored immediately after a disruption to ensure the company's ability to protect its assets, meet its critical needs and satisfy mandatory regulations and requirements. The following processes have been deemed Critical/Tier 1 for <District Name Here>:

- <Bullet List of critical business processes here>

3.3 Third Party Solutions and Products

Third-Party Solutions and Products include third-party software, hardware, or infrastructure that is developed, maintained, and/or hosted outside of <District Name Here> which either: processes, stores, transmits or receives information; and/or connects to the <District Name Here> network for the transmission or reception of <District Name Here> data. Third-Party Solutions and Products includes cloud-based and open sourced solutions, such as IAAS, PAAS, SAAS and XAAS.

4 Roles & Responsibilities

4.1 Chief Information Security Officer

Senior-level executive responsible for establishing enterprise vision, strategy, and security program at <District Name Here>

4.2 TPRM Program Manager

Responsible for managing TPRM Program, policy and standards, including identification of security controls, risk ranking methodology, risk stratification, due diligence, ongoing monitoring, kick off and coordination of risk third-party assessments, managing external audit team(s), reporting, and making recommendations for remediation and risk mitigation and program improvement. Responsible for conducting TPRM intake and assigning risk ranking for new and renewing Service Providers. Where applicable, TPRM Program Manager is also responsible for communicating remediation plans and timelines to <District Name Here> Legal.

4.3 Assessment Team Members

Responsible for conducting Service Provider assessments and corresponding with service providers on questions and responsive deadlines, compiling audit findings reports.

4.4 Sourcing

TPRM Program Manager shall partner with Sourcing to maintain a master list of qualifying Service Providers and data attributes.

4.5 Service Provider Relationship and <District Name Here> Technical Program Managers

Identified for new and renewing Service Providers and responsible for managing business relationship throughout the engagement at <District Name Here> In the event of a Relationship Manager and/or Technical Program Manager leaving their role, the department's Supervising Manager shall be responsible for designating a replacement.

4.6 InfoSec Compliance

Responsible for performing a review of PCI service providers during TPRM intake.

5 Risk Ranking Methodology

5.1 Data Classification & Risk

There are certain types of data which have been identified by <District Name Here> as inherently higher risk for sharing with Service Providers, including: personally identifiable information (name, address, SSN), sensitive personal information (credit card, protected health information or that identifies someone's race, ethnicity or religion), legally restricted information (attorney-client privilege, attorney work product, compliance reports), finance and accounting (sales revenues/budgets/forecasting, stockholder information, executive personnel changes, investment strategy) and InfoSec data elements (encryption keys, answers to security questions, access codes.)

Refer to <District Name Here> Data Classification Policy for complete list and details.

Additional factors such as how the data is accessed and/or what is being done with it, as well as the geolocation of the Service Provider and/or customer data may also increase the inherent risk of the third-party engagement.

5.2 Service Provider Risk Ranking

TPRM shall assess Service Provider attributes and assign a risk ranking as indication of Service Provider's level of risk. The risk ranking shall dictate TPRM strategy for ongoing monitoring and review of Service Provider.

TPRM risk ranking shall take into account a number of risk factors, including but not limited to:

- Inherent Risk (i.e., what type of data does service provider have access to, where is data stored and what's level and likelihood of harm that could result from breach);
- Risk Assessment Score(s) (i.e., how has service provider performed throughout the life of the engagement; and
- Vendor Health, Profile and Liability Thresholds (i.e., what is service provider's maturity level, geolocation and potential liability for breach.)

TPRM will assign an initial risk ranking of either high, medium or low risk, depending on the data type, data/network access and the industry/company maturity/geolocation in the chart, below. The Service Provider's risk ranking may be increased or decreased during the life of the service engagement to account for a high-level or compliance or non-compliance with security controls.

Risk Level	Data Type	Data/Network Access	Company Maturity/Geolocation
High	Tier 3 & 4 Data (pursuant to Data Classification Policy)	Customer/Employee Databases; Financial Systems; Critical Systems/Infrastructure	Start-Up; Global Cloud Services; China/EU/CA; Industry Regulated (PCI)
Medium	Tier 2 Data (pursuant to Data Classification Policy)	Privileged Reports; Privileged User Access; System Administrative Access	Industry Regulated (non-PCI)
Low	Tier 1 Public Data (pursuant to Data Classification Policy)	Intranet Systems	Publicly Certified Providers

6 Due Diligence

6.1 TPRM Intake

TPRM Program shall perform due diligence of all Service Providers, commensurate with the risk level, both at contract intake for all new vendors and at contract renewal for all existing vendors.

TPRM Program shall utilize an intake questionnaire which must be completed by business manager and Service Provider and provided to TPRM Manager. A Service Provider Relationship Manager and <District Name Here>Tech Technical Program Manager shall be identified for all new and renewing Service Providers. TPRM Managers shall leverage the information provided by Service Provider, <District Name Here> Relationship Manager, Technical Program Manager and Strategic Sourcing Manager in the response to questionnaire and shall ask additional follow-up questions, as necessary to complete Service Provider intake.

Prior to completing TPRM intake, if there have been security issues identified and/or remediation plans agreed upon by Service Provider as part of InfoSec Early Engagement, TPRM Manager shall communicate this information to <District Name Here> Legal who shall daft contractual terms/timelines for that remediation.

The TPRM review and intake shall be documented in Sourcing's Contract Lifecycle Management CLM tool as well as InfoSec's Governance Risk and Compliance GRC tool, which shall be used by TPRM to manage Service Provider list and manage TPRM ongoing monitoring (audit, assessment and self-attestation.)

The purpose of TPRM intake is fourfold:

6.1.1 Service Provider Profile and Risk Ranking

TPRM program shall use the information collected to assign a Service Provider profile and risk ranking, which shall inform level of scrutiny and ongoing monitoring throughout the entire engagement at <District Name Here>.

6.1.2 Data Protection Terms

As part of its due diligence, InfoSec shall assess level of risk and recommend that Service Providers with access to Tier 3 or 4 (see Data Classification Policy, above) and/or with access to <District Name Here> systems, be required to agree to <District Name Here> data protection terms. This recommendation will be made to Legal, which has final authority over the terms and inclusion of same in the agreement with Service Provider.

6.1.3 Implementation and Integration

Prior to granting a Service Provider access to <District Name Here> data or networks, TPRM Assessment Team Members shall refer the Service Provider Relationship Manager and Technical Program Manager to InfoSec's Information Security Policies and Standards, and instruct the Service Provider Relationship Manager and Technical Program Manager to comply with the policies relevant for the integration. Where a Service Provider Relationship Manager or Technical Program Manager is aware that a product or service has been implemented in a way that exposes <District Name Here> systems to a potential security incident, they must report that risk to InfoSec for review.

7 Ongoing Monitoring

7.1 Security Controls Assessments

Ongoing Monitoring for TPRM shall require the continual assessment of a Service Provider's security controls. Assessments may be conducted remotely or on-site. On-Site assessments shall require consultation and approval of <District Name Here>'s Legal Department.

An external Audit Team shall be used to conduct audits and provide findings reports to TPRM Manager. Timing for on-site assessments shall be coordinated and performed by external Audit Team.

7.2 Process for Conducting Controls Assessments

7.2.1 Kick-off Call

To kick-off an on-site or remote assessment, TPRM Program Manager shall notify <District Name Here> Service Provider Relationship Manager and Technical Program Manager of the need for an assessment. Relationship Manager shall coordinate an introduction and kick-off call with the Service Provider's point of contact. At the conclusion of the kick-off call, Service Provider shall be given a copy of, or access to, the TPRM controls assessment and a deadline for responses shall be set. At the discretion of the Assessment Team, Service Providers may provide appropriate documentation of security controls (e.g. SOC reports) in lieu of completing the TPRM controls assessment.

7.2.2 Assessment Team(s)

TPRM assessments shall be conducted by an Assessment Team. During the assessment, the TPRM Assessment Team shall work directly with Service Provider to any answer questions that may arise and to conduct follow-up requests for additional information or documentation, as necessary. Assessment Team shall monitor the response of Service Provider to ensure timeliness and shall follow-up and/or escalate to TPRM Program Manager if responses are past-due.

7.2.3 Assessment Reports

Upon submission of a completed response and supporting documentation by Service Provider, Assessment Team shall prepare and present an Assessment Report for InfoSec.

7.2.4 Review with Product Security Team

TPRM Program Manager shall review the findings with the InfoSec Product Security Team or TPRM Audit Team to determine if remediation is required.

7.2.5 Share Findings Meeting with Stakeholders

Based on the outcome of the Assessment Report meeting, TPRM Manager shall schedule a meeting with stakeholders to share the findings and determine if any compensating controls are available.

7.2.6 Draft of Final Report for Feedback

At the conclusion of the initial meeting to share assessment report with all stakeholders, a draft of the Final Report shall be compiled by TPRM Manager to allow for additional stakeholder feedback.

7.2.7 Final Report Published

Once all feedback has been received, a Final Report shall be published and shared with all stakeholders, including but not limited to, Legal, Strategic Sourcing, InfoSec and Service Provider Relationship Manager.

7.3 Remediation of Non-Conformities and Security Issues

TPRM assessment results shall be documented in a system of record to be maintained by InfoSec and the Service Provider's risk score shall be updated as a result of the assessment findings, as necessary. Security Issues that are detected as a result of the security assessments shall be documented.

InfoSec shall provide a report and recommendation to Service Provider and Relationship Manager of any issues which require remediation.

Remediation efforts shall be monitored and reported to stakeholders by InfoSec.

8 Payment Card Industry Standards PCI

8.1 Intake and Responsibility Matrix

All PCI Service Providers must be reviewed, and a risk analysis shall be performed prior to establishing a formal relationship with <District Name Here> As a requirement for onboarding, Service Provider must provide a competed PCI Attestation of Compliance (AOC) report, and PCI Responsibility Matrix (where applicable).

8.2 List of PCI Service Providers

As part of its ongoing monitoring, TPRM shall maintain a list of all qualifying Payment Card Industry PCI Service Providers which includes a description of the service provided, as there are a number of additional requirements which apply to PCI Service Providers and which shall be managed by TPRM Program. The PCI Service Provider list shall be maintained in Excel and updated quarterly. However, work is underway to automate the list in a tool available to InfoSec and/or Strategic Sourcing Teams.

By definition, PCI Service Providers shall include all provides which are not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity and includes companies which provide services that control or could impact the security of cardholder data.

8.3 PCI Data Protection Terms

TPRM shall recommend to Legal that all qualifying PCI service providers agree to the Data Protection Terms, which must include, at a minimum, an acknowledgement that the service providers are responsible for the security of cardholder data that the service providers possess or otherwise store, process or transmit on behalf of <District Name Here>, or to the extent that they could impact the security of the <District Name Here>'s cardholder data environment.

8.4 Annual Monitoring of PCI Service Providers

The Service Provider's PCI DSS compliance status shall be monitored by TPRM on, at least, an annual basis.

9 Cadence for Ongoing Monitoring & Review

The Service Provider's residual risk ranking shall determine the cadence for ongoing monitoring and assessment of Service Provider, as described in the chart below.

Generally, security assessments shall be performed every 9-12 months for high risk rankings or every 18-24 months for medium risk rankings. Service Providers with a risk rank of low shall only be required to provide bi-annual self-attestation of compliance, unless circumstances dictate otherwise. Greater frequency of review may be ascribed, depending on the circumstances and level of risk.

Residual Risk	Frequency
Critical/Data Breach	ASAP
High	9-12 months

Medium	18-24 months
Low	Bi-Annual Self-Attestation

10 Common Controls Framework

TPRM assessments shall leverage the <District Name Here> Common Controls Framework CCF controls identified for TPRM and shall be tailored depending on service provider's services and level of risk.

11 TPRM Key Performance Indicators KPI

TPRM Program shall provide regular reporting on the performance of TPRM Program to CISO and other Program stakeholders, which may include but is not limited to the following:

- TPRM audit volumes (active/ongoing and completed)
- TRPM audit and/or testing results
- Security issues identified and resolved through TPRM (remediation)
- Risk acceptance for issues uncovered by TPRM
- Trends (issues, remediation, risk acceptance)
- Performance Improvements resulting from TPRM issue identification
- GRC/TPRM Tool – reporting available (TBD)
- Active vendor list – link to database with vendor profiles (and/report on progress to completion)
- Integration with <District Name Here> Enterprise Vendor Management Processes and/or blockers identified
- Cost of TPRM

12 Approval and Effective Date

Effective Date will be **<Effective Date Here>**

APPROVED BY _____ Date _____

<Approver Name Here>

13 Document History

A record of policy revisions is maintained in the following table:

Date	*Revision*	*Description*	*Author*	*Approver*