Formōs
Consulting

# Cybersecurity Considerations in Third Party Risk Management

# TPR Definition & Scope

- Third-party risk is the potential for loss, disruption, or harm to an organization that arises from its relationships with external entities such as **vendors, suppliers, contractors, service providers, or business partners**.
- TPR frequency arises from outsourced services or an outsourced function.
- TPR originates from providing access systems or data, or from the responsibility to deliver goods or services.

Formōs
Consulting

# Why Should We Care About Third-Party Risk Management?

# Reasons to Care About TPRM

- **30%** of Data Breaches originate from third-party vendors[1]
- Effective TPRM is necessary to meet regulatory requirements (HIPAA, GLBA, PCI DSS, etc.)
- Effective TPRM is necessary to meet contractual requirements with vendors and customers

Formos Consulting

[1] Verizon's Data Breach Investigations Report (2025)

# Oldies, But (Not So) Goodies

# Target Breach (2013)

- Breach occurred through Target's Third-Party HVAC Company
- Obtained HVAC employee's credentials to Target's Web Portal
- Used a vulnerability in Web Portal to elevate admin privileges
- Installed Malware on Point-of-Sale (POS) terminals
- 40 million payment cards were stolen
- Nearly $300 million in estimated losses

# Target: Lessons Learned

- Even the “lowest risk” third-parties carry risk
- Due diligence is required

# SolarWinds (2020)

- Attacker injected malicious code into Orion Platform, the software used by customers to monitor their IT devices
- Malicious code was deployed to thousands of customers as part of routine update.
- When customers installed the update, it activated a backdoor in their system.

Formōs Consulting

Formōs
Consulting

# TPRM Frameworks & Guidance

# Relevant TPRM Frameworks & Guidance

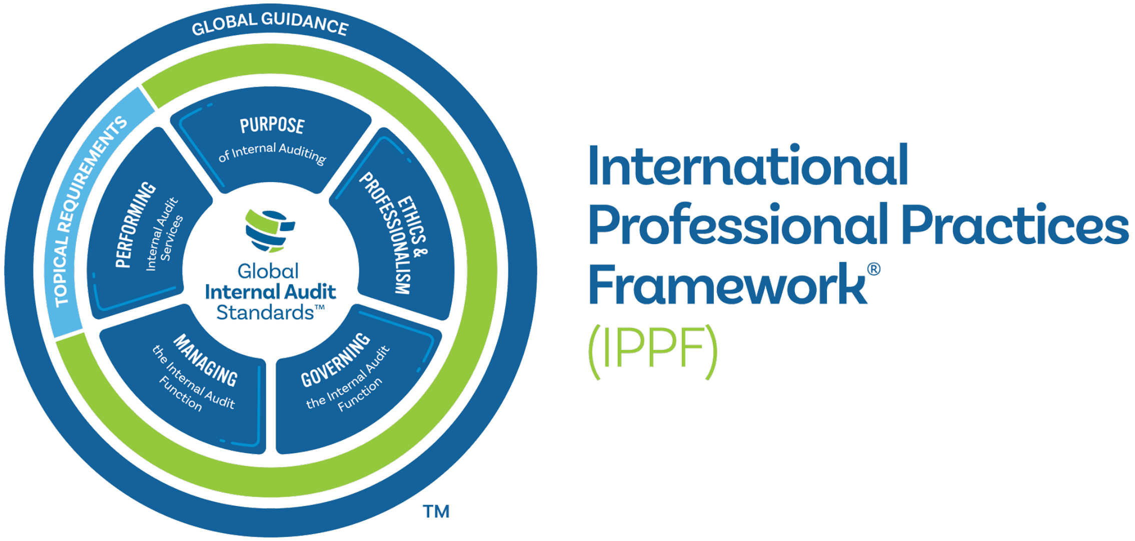
- **NIST CSF 2.0**
- ISO 27001:2022
- COSO
- **IIA’s Third-Party Topical Guidance**

# NIST CSF 2.0

- Released February 2024 (first update since 2014)
- Added the “Govern” function
  - Blueprint for TPRM governance
- Can map organization’s TPRM program to the CSF 2.0 categories

# IIA’s Third-Party Topical Requirement

- Effective September 2026
- Aligned with frameworks such as ISO 27001, GDPR and HIPAA
- Outlines TPRM Lifecycle
- Divided into three sections:
  - Governance
  - Risk Management
  - Controls


GLOBAL GUIDANCE
TOPICAL REQUIREMENTS
PURPOSE of Internal Auditing
ETHICS & PROFESSIONALISM
GOVERNING the Internal Audit Function
MANAGING the Internal Audit Function
PERFORMING Internal Audit Services
Global Internal Audit Standards™
TM
International Professional Practices Framework®
(IPPF)

Formōs
Consulting

# TPRM Software & Tools

# TPRM Software/Tools

- Variety of options for managing third-parties:
  - Dedicated TPRM Solution
  - IT Service Management (ITSM) / Ticketing System
  - Excel Spreadsheets / File Shares
- The best choice will be dependent on the needs of your organization based on the number of total third parties, the risk they pose, and other critical factors.

# Dedicated TPRM System

- Can manage the entire vendor lifecycle (vetting, RFP/screening, onboarding, ongoing monitoring, renewal/termination, etc.)
- Often has automated functionality, saving manual efforts
- Comprehensive reporting abilities
  - Dashboards
  - Detailed reports
- Expensive

# IT Service Management System

- Might already have the platform in place, saving time and money to implement
- Can build workflows and approvals into the platform
- Not built specifically for TPRM, so will have limitations around dashboards, reporting, etc.

# Spreadsheets / File Shares

Tracking Vendor(s) and Related Information (accounts, system accounts, APIs, etc) via spreadsheet:

- Free!
- Ideal for environments without a significant number of unique vendors
- Limited functionality and reporting

# Relevant InfoSec Tools

| InfoSec Solution | Vendor Example | Role in TPRM |
|---|---|---|
| Identity & Access Management (IAM) | Okta, CyberArk, Microsoft Entra ID | Monitor TP Users and Activity; ensure full Decommissioning |
| Privileged Access Management (PAM) | CrowdStrike, CyberArk | Approvals to gain admin access; time limitations to admin access; least privileged enforcement; password rotations, etc. |
| SIEM / Log Aggregators | Splunk, SumoLogic | Monitor TP user activity |
| ITSM | ServiceNow | Gain approvals prior to granting admin access |
| Data Loss Prevention (DLP) | Symantec, ForcePoint | Prevent loss of sensitive data |

** need to understand how each solution supports control objectives; consider auditing the scope and configuration of each toolset as well as the result of monitoring activities

Formōs Consulting

Formōs
Consulting

# TPRM Best Practices

# TPRM Best Practices

1. TP Governance & Policies
2. Stratify TP users based on risk; deploy appropriate controls for each
3. Stratify TP organizations based on risk
4. Log TP user activity – application layer, database layer, OS/command line
5. Certify/recertify TP users routinely / forced end-dates for TP users
6. Flag TP users separate from EE users – consider HR systems or IAM
7. Prompt decommissioning process for TP users
8. Least privileged access for TP users
9. Multifactor Authentication for TP users

# TPRM Best Practices

10. TP Contract provisions which address:

- Right to Audit
- Limitations of Liability
- Required Compliance with Standards (with Reporting) – SOC, HITRUST, etc
- Security Questionnaires
- Right to Pen Test (limited restrictions on scope)
- Notification Requirements (employee terms, key position turnover, suspected breach, etc)
- Required Security Protocols, in the event of trusted networks, dedicated connections, regulated data sharing etc.
- Require Security Policies (no offshore for regulated data, use of contractors, written acknowledgement of security policies, etc)

Formōs
Consulting

# TPRM Lifecycle

# Third-Party Lifecycle / Phases

## 1. SELECTION

Determining the need, plan for use, and **due diligence** for selection.

## 2. CONTRACTING

Drafting, negotiating, approving, and implementing legal agreements.

## 3. ONBOARDING

Contract is signed. Bringing the third-party onboard

## 4. MONITORING

Progress is monitored, and any deviations from the plan are identified and addressed.

## 5. OFFBOARDING

Ending contracts and agreements. Maintaining the exit strategy with a formal exit plan.

Formōs
Consulting

# Phase 1: Selection

# Third-Party Risk Assessment / Due Diligence

- Goal is to evaluate the risks posed to your organization by the third party, both for *inherent risk* and *residual risk*.
- Might use an internally developed template/questionnaire to help identify the controls and risks.
- Using the results from the risk assessment and due diligence, we can classify third-parties into Categories/Tiers (e.g. high, medium, low).

# Third-Party Risk Assessment: Factors

- Inherent Risk
  - What types of data/access does the third-party have?
  - Criticality/Importance of third-party to our company (dollar amounts, volume of activity, regulatory requirements, etc.)
  - Industry / Nature of business

- Residual Risk / Controls
  - Third-party assurance (SOC reports, PCI, ISO, HIPAA)
  - Business Continuity / Disaster Recovery
  - Financial Stability
  - Recent breaches or known threats?

# Third-Party Risk Assessment: Key Points

- The amount of due diligence required is driven by the inherent risk / risk profile of the third party.
- Don’t ignore the risk assessment results!
  - Only 29% of companies remediate risks found during the vendor sourcing and selection stage. (Prevalent)
  - There’s no point in performing the risk assessments and due diligence if it isn’t going to meaningfully impact decision making in the selection process.

# SOC Reports

- Are generally helpful in providing some assurance regarding the third party's control environment.
  - Might be limited in its scope
  - Might have testing exceptions / qualified report
  - Quality of report might be lacking.
- Cannot blindly place full reliance on the fact that a third party has a SOC report.

Formōs
Consulting

# Phase 2: Contracting

# Request for Proposal (RFP)

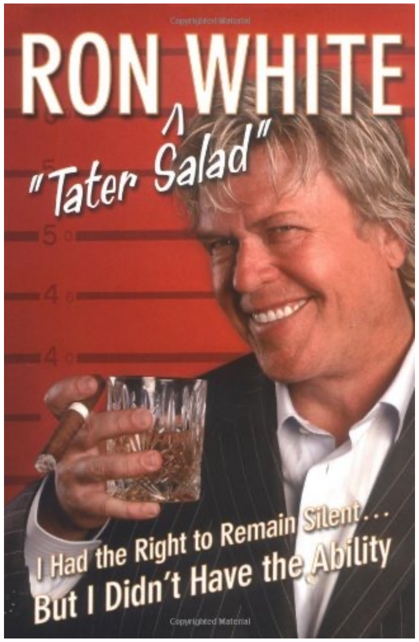
- To weed out potentially problematic/noncompliant third parties, you should include the key provisions to address TPR within the contract requirements in the RFP.
- TPR requested provisions are ideally addressed in selection/ RFP process.  Worst case in the contracting process.  This true for situations where the TPR arises from a partner relationship or an independent contractor and may not otherwise follow the new vendor scrutiny, including InfoSec evaluation.

# Contracting

- Make sure to consider including the following in your contracts with third parties:
  - Responsibility for information security and privacy
  - Data ownership
  - Scope / Timing
  - Right to Audit
  - Service Level Agreements (SLAs)
  - Terms upon termination of contract (related to assets/data)

# Right to Audit

- Gives you the RIGHT to audit (not required)
- Should be included in the third-party contract/BAA/etc.
- Should clearly define terms:
  - How frequently it can be performed
  - How much advance notice is required
  - Scope of audit/procedures
  - Who will be performing the audit
  - Who's responsible for paying for audit


RON "Tater Salad" WHITE
I Had the Right to Remain Silent...
But I Didn't Have the Ability

Formōs
Consulting

# Right to Audit Examples

- Lack of third-party assurance
- SOC report has a limited scope (e.g. doesn’t include business continuity or disaster recovery)
- SOC report had exceptions identified
- Recent breach/incident

# What To Do if We Cant Get “Right to Audit”

- Evaluate our company’s risk appetite
- Evaluate third party’s overall risk profile
- In some instances, could be determining factor in the selection of a third party

# Service Level Agreement (SLA)

- Sets the expectations/requirements between the customer and third party (service provider)
- Should be as clear/descriptive as possible to avoid potential misinterpretations or disputes
- Should be reviewed periodically as part of the “Monitoring” stage

CDK Global
CDK
Global®

# CDK Global Breach

- Ransomware attack impacting North-American Car Dealerships
- Dealerships had to use pen and paper for weeks
- In addition to systems being down for several weeks, sensitive data was compromised.

# CDK Global Lesson: Inadequate MSA/SLA

- Promised "Reasonable Security Measures"
- No explicit service-level guarantees
- Agreement's capped CDK's liability for any claims regardless of cause at the lesser of:
  - The actual damages incurred by the dealer, or
  - *One month's worth of the average fees paid to CDK*
- Explicitly excluded CDK from liability for lost profits or business interruption damages under any circumstances!

Formōs
Consulting

# Phase 3: Onboarding

# Onboarding

The third-party onboarding process needs to address at least the following areas:

- Policies, Training, & Security Awareness
- Access Controls
- Security Controls

# Policies, Training, & Security Awareness

- Third-Parties should be treated similarly to employees in the requirement to read/acknowledge company policies as well as complete applicable training
- Where possible, should be required at the third-party employee (individual) level as opposed to global/vendor-wide.

# Access Controls

- Least Privilege
  - Access should be granted only to the level its required
  - Often ignored in favor of convenience ("Might need it someday")
- **Multi-Factor Authentication (MFA)**
  - Should be required for all vendor access
- Set Access Expiration Dates
  - Can always be extended as needed, but force someone to manually review to do so

# Access Controls (Continued)

- Access Reviews
  - Company: Company is reviewing to identify inactive third-parties
  - Third-Party: Third-party is reviewing to identify their own employees who no longer required access.
- Terminations
  - Ensure there's a process in place to remove access for third-party employees who are terminated.

# Security/Technical Controls

Will vary the most by company and vendor relationship, but the following will generally apply:

- Data Encryption (at rest & in motion)
- TP Pen Tests / Web App Pen Test / Vulnerability Assessments
- Business Continuity & Disaster Recovery

Formōs
Consulting

# Phase 4: Monitoring

# Third-Party Monitoring

- Arguably the most neglected stage of the TPRM Lifecycle
- Only **14%** of companies perform true continuous monitoring of their third-parties[1]
- Less than half (**46%**) strongly believe their monitoring program is meeting contractual and regulatory requirements. [1]
- Only **27%** of the total risk management effort is allocated to ongoing monitoring over the course of the relationship. [2]

Formōs Consulting

[1] Risk Management in a Technology-Driven World, Supply Wisdom (2024)

[2] Need to update this source.

# Ongoing Third-Party Monitoring

- Not a “Set it and forget it”
- Must be constantly evaluated to ensure that risks are addressed as changes occur to the third party, applicable regulations, industry conditions, and other relevant factors.

# Ongoing Third-Party Monitoring

- Should be looking for the following:
  - Changes in the nature of the relationship/scope
  - Gaps in meeting SLA
  - Gaps identified in assurance efforts (SOC reports, etc.)
  - Acquisitions / Changes to org structure
  - Financial instability
  - Breaches / Information Security issues
  - Industry/Environmental changes

# Creative Ongoing Third-Party Monitoring

- Monitoring Social Media Accounts
- Monitoring Message Boards
- Monitoring the News
- Looking at Quarterly Filings
- Monitoring/Identifying "Fourth Party" Relationships

# Periodic Risk Assessments / Audits

- Need to start with all third-parties and then can exclude/prioritize during the assessment process.
- Can't assume that the risk profile hasn't changed since the last risk assessment or audit has been completed.
- Results will help us identify the areas of highest risk so we can prioritize our time and resources towards them.

Formōs
Consulting

# Phase 5: Offboarding

Formōs
Consulting

# Third-Party Offboarding

- Along with Monitoring, arguably the most neglected stage of the TPRM Lifecycle
- Only 14% of companies use true continuous monitoring of their third-parties[1]
- Less than half (46%) of companies strongly believe their monitoring program is meeting contractual and regulatory requirements. [1]

[1] Risk Management in a Technology-Driven World, Supply Wisdom (2024)

# Offboarding Concerns: Removing Access

- Must remove/disable all accounts timely
  - Individual accounts
  - **System/Service accounts**
- API Keys & Integrations must be disabled

# Offboarding Concerns: Data Retention

- Data must be returned, destroyed, or retained based on:
  - Regulatory requirements
  - Contractual requirements
  - **Audit requirements**
- Retaining audit evidence isn't generally the focus, but should be considered to ensure it isn't lost.

# Thank You!

Questions?

Taylor Ezell, CISA, CISSP, CPA
Sr. Manager, IT Risk and Compliance

taylor.ezell@formosconsulting.com
Cell: 615.300.3567

Formos
Consulting