Auditing Third Party Risk Management Programs

ISACA/IIA San Diego IT Seminar
April 12, 2018

Presented by
Zachary Couasnon, RiSK Opportunities, Inc.

Business & IT Advisory
Processes & Controls
Governance & Risk
Internal Audit
Compliance

RiSK Opportunities

The Institute of Internal Auditors

ISACA

Discussion Points

Introduction

- What is a Third Party?
- 3 Brief Third Party Case Studies
- Why do we need Third Party Risk Management (TPRM) Programs?

TPRM Assessment Process (Nuts & Bolts)

- Parties involved
- Vendor Onboarding Process
- Vendor Risk Assessment Process

Discussion Points, continued

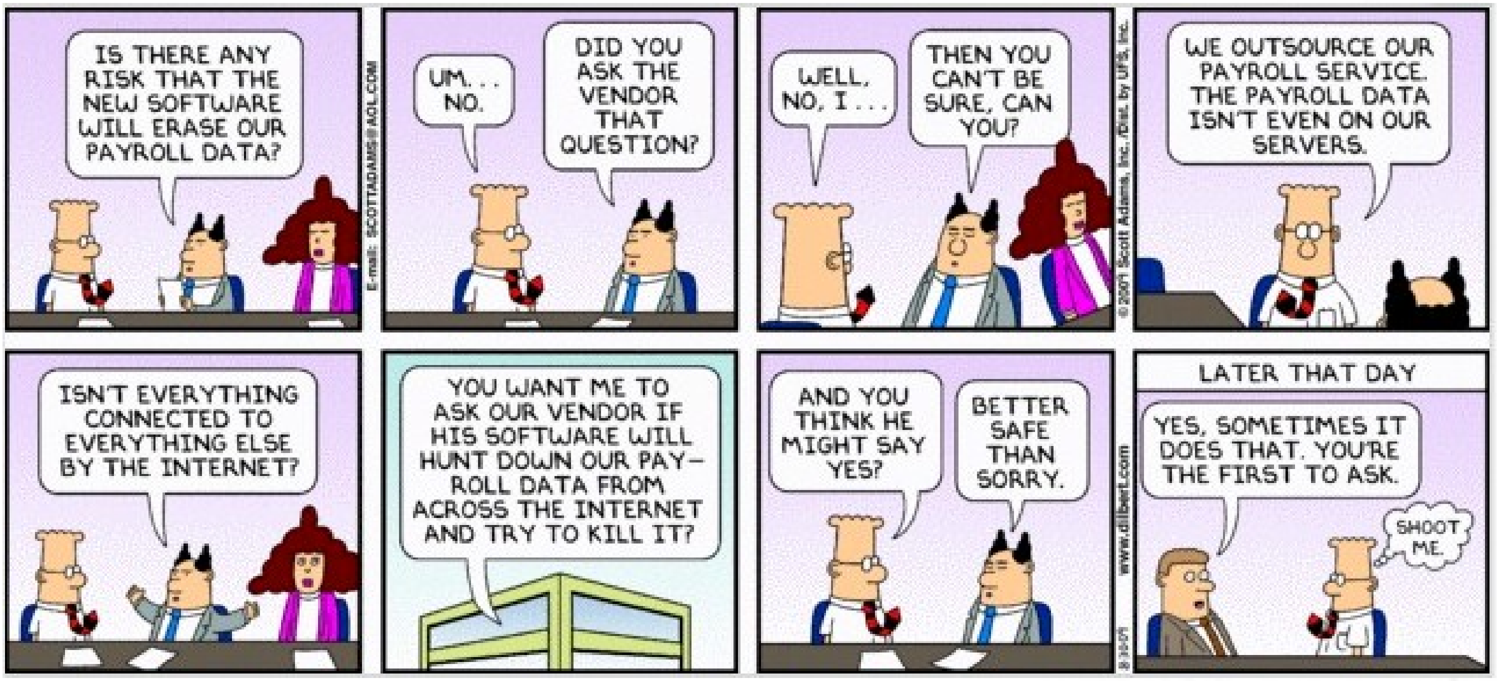
TPRM Maturity Models

- NIST PRISMA based approach

Auditing TPRM Programs

- Audit scoping recommendations
- Functional approach walkthroughs (example)

Questions & Feedback


IS THERE ANY RISK THAT THE NEW SOFTWARE WILL ERASE OUR PAYROLL DATA?
E-mail: SCOTTADAMS@AOL.COM
UM. . . NO.
DID YOU ASK THE VENDOR THAT QUESTION?
WELL, NO, I . . .
THEN YOU CAN'T BE SURE, CAN YOU?
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
WE OUTSOURCE OUR PAYROLL SERVICE. THE PAYROLL DATA ISN'T EVEN ON OUR SERVERS.
ISN'T EVERYTHING CONNECTED TO EVERYTHING ELSE BY THE INTERNET?
YOU WANT ME TO ASK OUR VENDOR IF HIS SOFTWARE WILL HUNT DOWN OUR PAYROLL DATA FROM ACROSS THE INTERNET AND TRY TO KILL IT?
AND YOU THINK HE MIGHT SAY YES?
BETTER SAFE THAN SORRY.
www.dilbert.com
LATER THAT DAY
YES, SOMETIMES IT DOES THAT. YOU'RE THE FIRST TO ASK.
SHOOT ME.

Introduction

- What are Third Parties?
  - Example 1:

    Problem: You work for a manufacturing company that makes really good widgets. However, your company does not make very good websites to sell the widgets.

    Solution: Hire a Web Developer to build a web storefront
  - Example 2:

    Problem: Traffic and sales on your new storefront are tremendous and now your company is a Tier 1 Merchant and must be PCI Compliant. PCI expertise is not in-house.

    Solution: Onboard a PCI Compliant processor to handle payments and a qualified QSA firm to assist with compliance.
  - Example 3:

    Problem: Traffic and sales are so tremendous your web storefront needs more bandwidth.

    Solution: Migrate the web storefront to the cloud for rapid on-demand scaling.

Introduction, continued

- What are Third Parties?
  - Simply, a Third Party is an external person or a company that provides a service to an organization not their own.
  - Service organizations types are vast
    - HR and Payroll (ADP)
    - Cloud Services (SaaS, PaaS, IaaS, AWS, Azure, Google, etc.)
    - Outsourced Legal
    - IT Datacenters, Helpdesks, Developers, DBAs
    - Professional service companies (Auditors, InfoSec Professionals)
    - OEM Manufacturing
    - Medical Service Providers (Quest Diagnostics)

Introduction, Crowd Survey

Would anyone like to name and describe Third Parties you interface regularly with at your company?

- Please include your name and your company in your response
- As incentive, I have candy for brave responders! ☺

Introduction, Case Study

- 2013 Target Breach (Cybersecurity)
  - Breach lasted from 11/27 to 12/15
  - 70M+ PII records were exposed
  - 40M+ credit and debit card numbers were exposed
  - Breach cost Target approximately $250M vs the estimated $54M in sales generated by the sale of the credit cards and PII on black markets.
  - CEO and CIO both resigned
  - Attackers gained access to the store network via HVAC systems managed by Fazio Mechanical Services, a third party.
  - HVAC systems had access to the store network so that vendors could remote in and maintain the HVAC systems.

https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company

Introduction, Case Study

PARKER DRILLING

- 2013 Parker Drilling (FCPA Impact)
  - In 2001, a third party called Panalpina was contracted to work with Nigerian Customs agents in regards reducing tariffs incurred for to their drilling rigs being exported to and from Nigeria.
  - Panalpina filed fraudulent paper work with Nigerian Customs and bribed officials to secure the success of the paperwork.
  - A Panel of Inquiry discovered the fraud and levied a fine of $3.8M against Parker Drilling in 2004
  - Parker hired another third party (law agency) to work with Nigerian Customs to reduce the fine amount. The contract was for $1.25M and much of the money was used to bribe Nigerian officials (again!)
  - As a result, the Houston based company paid out $15.85M in penalties and settlements to the US DOJ, SEC, and Nigerian Customs after an investigation in 2013.

http://www.fcpablog.com/blog/2013/4/16/parker-drilling-in-1585-million-settlement.html

Introduction, Case Study

- 2018 Facebook / Cambridge Analytica (Privacy, Compliance, Company Profile)
  - 2014 CA hired a researcher to gather basic profile information of Facebook users
  - App called This Is Your Digital Life performed surveys for 300K Facebook users along the lines of what the user "liked"
  - EXCEPT that the app also pulled in data for 50-87M other users ("privacy settings")
  - Data was passed to CA and who effectively created "psychographic" targeting and modeling strategies for ad campaigns
  - CA told Facebook the data was destroyed but this is a highly questionable claim
  - Facebook shares dropped 18% after March 17th.
  - #DeleteFacebook movement

http://fortune.com/2018/04/10/facebook-cambridge-analytica-what-happened/

Introduction, Summary

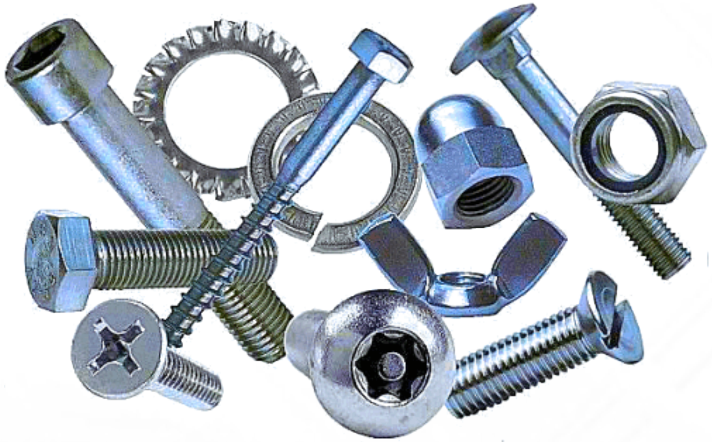
- Third Parties comes with an amount of risk that could adversely impact the contracting organization
- The practice of Third Party Risk Management (TPRM) is the process of analyzing and controlling risks presented to your company by external parties with which your company has a business relationship.
- Risks introduced include IT InfoSec, legal, privacy, compliance, operational, financial, and business image risks.

Introduction, Summary

- These risks needs to be ***qualified***, ***quantified***, ***tracked***, and ***mitigated*****.**
- Unfortunately, there are no frameworks such as ISO, NIST, CoBIT, etc. which explicitly govern TPRM. However, we can leverage the risk assessment guidance these frameworks provide.

TPRM Assessment Process, Nuts & Bolts

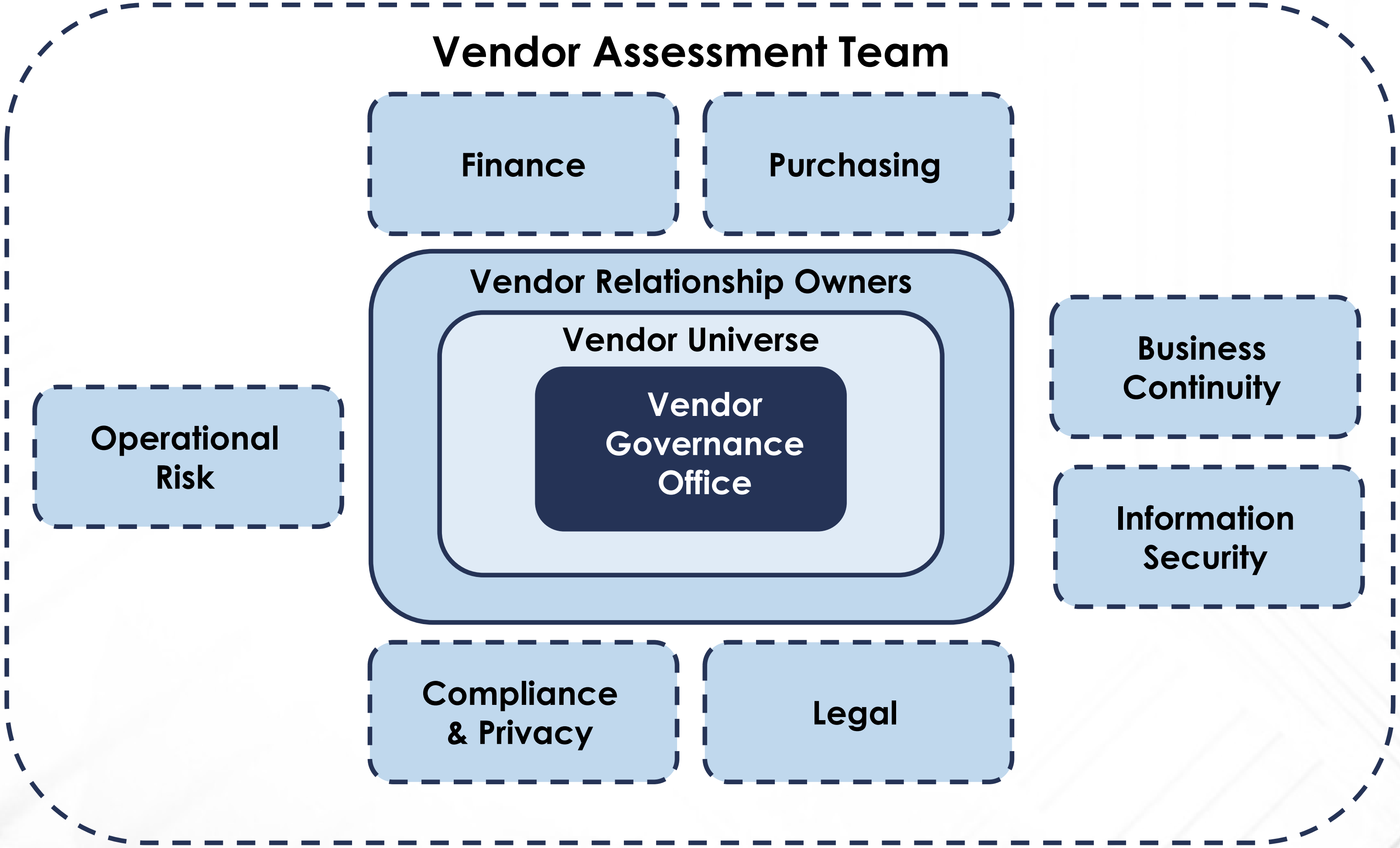
- **This section:**
  - Examine key business organizations involved in the TPRM process
  - Review the “generic” Third Party Onboarding process
  - Walkthrough the Vendor Risk Assessment Process (5 Steps)
- **Up next:** TPRM Maturity Models



TPRM Assessment Process, Key Orgs

- Understanding business organizations that are key in the onboarding process will help scope the audit and isolate control activities.

TPRM Assessment Process, Key Orgs



www.nicsa.org / https://www.slideshare.net/nicsaonline/thirdparty-risk-management-implementing-a-strategy

TPRM Assessment Process, Key Orgs

- Business users who want to onboard the Third Party (Finance, Operations, HR, Legal, IT, Marketing, Facilities, etc.)
  - These are your **BROs (Business Relationship Owners)**
- Procurement
  - Critical organization – coordinates onboarding activities with BROs, Vendors, Legal, IT, Finance, and any other impacted organizations
  - Be good friends with these people ☺ They know everyone!
- Risk Organization
  - Organization placement varies. Can be a subset of IT or maybe part of a larger global risk function.
  - Vendor Governance Office (ownership of the assessment process)

TPRM Assessment Process, Key Orgs

- Legal Team
  - Handles Contracts, NDAs, SOWs, and MSAs as they are fluent in legalese
- Privacy Team
  - Often part of the legal team, they specialize in privacy and are extremely important if the Third Party handles employee and/or customer PII
  - Major players in the GDPR space – impacts US companies with European customers
- BCM Team
  - Become important during the assessment process if the Third Party is very critical to company operations
  - Example: HR wants to onboard a Third Party to manage Payroll

TPRM Assessment Process, Key Orgs

- Finance & Accounting
  - Manage the budgeting and Accounts Payable components of onboarding a Third Party
- IT (Product Security & Governance)
  - IT will perform a technical risk assessment of the vendor's product in tandem with the vendor assessment (sometimes efforts overlap)
  - Example: HR wants to onboard a cloud based benefits vendor. TPRM will assess the vendor, Product Security will assess security aspects of the cloud platform (such as encryption standards for data in transit and at rest).

TPRM Assessment Process, Top Level Goals

- The amount of effort and due diligence performed during a Third Party Assessment should match the level of risk the vendor brings to an organization.

- A successful assessment will provide Management with reliable information to make an informed decision in regards to onboarding the Third Party.

- Vendor Risk Assessment 5 Steps
  1. Vendor Risk Appraisal
  2. Due Diligence
  3. Risk Assessment and Mitigation
  4. Monitoring and Reporting
  5. Recertification Management

TPRM Assessment Process, Appraisal

- Step 1: Vendor Risk Appraisal
  - The appraisal process must be consistent and repeatable
  - Appraisal process considers 3 types of risk
    1. Inherent/Relationship Risk to the Organization
       - These risks are incurred as a direct result to onboarding
         - Compliance & Regulations
         - Data driven privacy risks
         - Financial
         - Continuity Risks
    2. Business Profile Risk
       - Company Stability
       - Credit Rating
       - Geopolitical

TPRM Assessment Process, Appraisal

- Step 1: Vendor Risk Appraisal, continued
  3. Controls Risk
     - These risks are driven by the Third Party's control environment
       - Unless you're planning to perform an independent audit on the Third Party's control environment, external assessments such as SOC1 & 2 Type 2, ISO, PCI ROC, etc. are a great way to get comfort around the vendor control environment.
  - In mature TPRM processes, these 3 risks are quantified into a vendor "score".
    - Example: Inherent/Relationship Risk (weight) + Control Assessment Risk (weight) + Profile Risk (weight) = Vendor Score
    - Vendor Score is derived from Appraisal and Due Diligence activities

TPRM Assessment Process, Diligence

- Step 2: Due Diligence
  - Actually performing the assessment
  - Procedures must be repeatable
  - Risk Assessments must be completed for all new contracts regardless of business organization
  - Many frameworks provide guidance for performing a risk assessment
    - Most operational – ISO 27005
    - Most technical – NIST FIPS 200 (Federal Information Processing Standards)
    - Most strategic – CoBIT
  - Due Diligence requires use of judgement and professional skepticism, the policy just defines the requirements.
    - "Doing what makes sense" for the vendor assessment, not just checking boxes

TPRM Assessment Process, Diligence Examples

- Vendor self-assessment surveys (most common)
  - Survey type is driven by appraisal risk
  - Example: Cloud Vendors should complete the CSA CAIQ (Cloud Security Alliance Consensus Assessments Initiative Questionnaire)
  - Archer and Keylight GRC tools use a self-assessment derived from Society for Information Management (SIM) Cybersecurity SIG (Subject Interest Group). SIG is a US based organization and is not as relevant for EU or Asian Corporations.
- On-site testing (expensive and legal barriers)
- Review of Service Organization Control (SOC) reports (Type 2)
  - SOC1 for SOX vendors (covers financial reporting controls)
  - SOC2 for Data Vendors (covers controls around security, availability, processing integrity, confidentiality, and privacy of a system)

TPRM Assessment Process, Diligence Examples

- Review of ISO Certifications
- PCI Report on Compliance (ROC)
- Inspection of vendor policies such as
  - Cybersecurity & IT
  - HR Policies (ex. New Hire Onboarding & Termination)
  - Incident Management
  - Change Management
  - Business Continuity and Disaster Recovery
- Inspection of
  - Most recent vulnerability and penetration tests
  - Most recent Business Continuity and Disaster Recovery testing

TPRM Assessment Process, Tiering

- A key deliverable from the Appraisal and Due Diligence steps is the Vendor Scorecard and Vendor Tier

- In some TPRM programs these are the same but there are advantages of keeping them separate.
  - Vendor Tiering is a way to "bucket" vendors based on specific types of risk
  - Scorecards are a way to "rank" vendors based on overall risk (3 aforementioned components)

- These two concepts can be formalized differently depending on the organization's needs but these principles should be baked into every TPRM program.

- Scoring and Tiering are auditable and the process should be repeatable.

TPRM Assessment Process, Assessment and Mitigation

- Step 3: Risk Assessment and Mitigation
  - Chances are there will be gaps/risks in the Vendors security and controls programs discovered during due diligence procedures
  - These gaps/risks must be reported, tracked, and mitigated
  - Mitigation Strategies for Third Party Gaps
    - **Do nothing**! (not really mitigation)
      - Business organization will accept the risk (should be written)
      - Issuance of an EtP (Exception to Policy)
      - Reported as such in Risk Registry
    - **Avoid** the risk
      - Exclude certain services provided by vendor that expose organization to unwanted risk
      - Not always feasible

TPRM Assessment Process, Assessment and Mitigation

- Step 3: Risk Assessment and Mitigation
  - **Remediate the risk**
    - The third party wants your organization’s business, use leverage and push for remediation
    - Include remediation items in the contract
      - Provides further leverage during contract renewal when discussing fees, etc.
    - Work with the vendor and agree on method of remediation
    - Set timelines for remediation and enforce them
    - Record the gap/risk in the Register and track to completion

TPRM Assessment Process, Monitoring and Reporting

- Step 4: Monitoring and Reporting
  - Documenting 3rd Party Risks in a Registry (Archer, Keylight, etc.)
  - Monitoring remediation deadlines
    - Working with the BROs, Legal, and Vendors to validate gaps/risks have been remediated in the agreed upon manner
  - Effectively reporting vendor risk landscape to management
    - Focusing on key vendors (most critical and with highest risk)
    - Upcoming remediation deadlines
    - Focusing on Critical/High Risks with the most impact
    - Performance Metrics
      - Assessment timeliness
      - Remediation goals
    - Escalation of past-due remediation for risks

TPRM Assessment Process, Monitoring and Reporting

- Step 4: Monitoring and Reporting
    - Documenting Due Diligence and Risks in Assessment Report
    - Reports should be concise
        - Summary of Inherent, Profile, and Controls risk
        - Tiering and Scoring rationale
        - Summary of Due Diligence performed
            - Inquiry with who? When? For what?
            - Should be in line with policy procedures
        - Identified Risks and impact should be detailed and ranked (usually C, H, M, L)
        - Evidence of review and approval of report by BROs and Risk Org (Signature Page)
        - References to supporting documentation

TPRM Assessment Process, Recertification

- Step 5: Recertification Management (effectively a detective control)
    - As time passes, trusted vendors tend to get more and more work from the organization and greater reliance is placed on rendered services.
        - This could potentially lead to changes in services rendered by the vendor not part of initial appraisal.
        - Changes in data types, dependencies, etc. are all factors
    - Based on Vendor Tier and Scorecard, vendors should be re-assessed on a set schedule
        - Critical or High Risk vendors – at least annually
        - Less critical vendors – Approx. every 2 years
    - TPRM being closely integrated with Procurement and Legal is the best way to detect changes in third party vendor services and trigger a re-assessment.

TPRM Maturity Models

- **This section:**
  - Review the NIST PRISMA approach to assessing the maturity of a Third Party Risk Management Program
- **Up next:** Auditing a Third Party Risk Management Program

I JUST READ THIS GREAT BOOK ABOUT HOW TO "REENGINEER" OUR BUSINESS PROCESSES.
UH-OH
EVERYBODY'S DOING IT. WE'D BETTER JUMP UNDER THE BANDWAGON BEFORE THE TRAIN LEAVES THE STATION! I'M PUTTING YOU IN CHARGE.
IF YOU NEED ANY MANAGEMENT SUPPORT YOU KNOW WHERE TO GO.
S.Adams E-Mail: SCOTTADAMS@AOL.COM
© 1994 United Feature Syndicate, Inc.
2-28

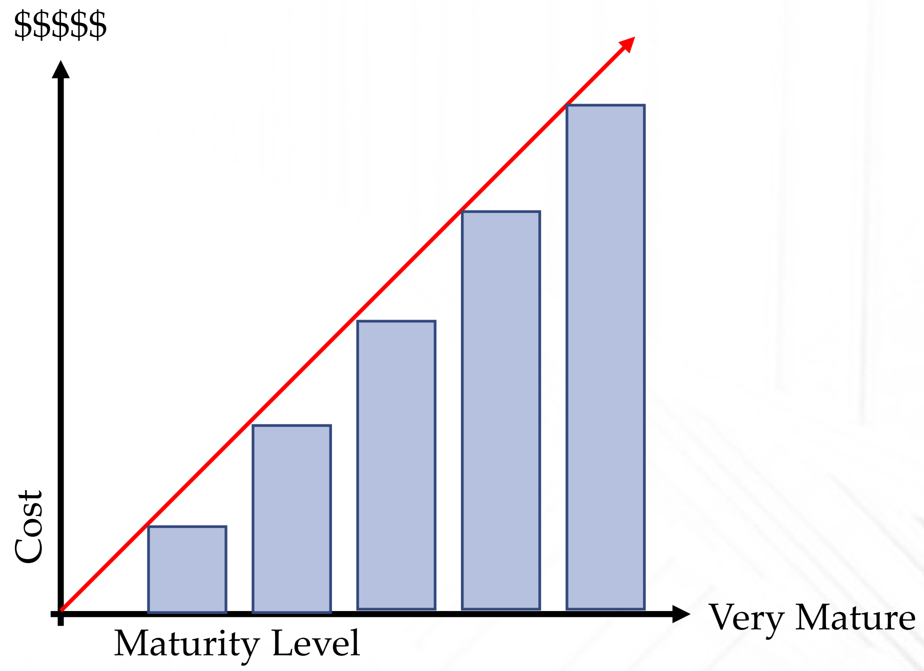
TPRM Maturity Models, Introduction

- It's important to understand how mature the TPRM Program is at your organization for audit scoping.
- Not all organizations need a fully mature TPRM Program
- Maturity Assessment/Levels in this presentation are based on the NIST PRISMA (Program Review for Information Security Assistance).
- Program was designed to
  - To assist agencies in improving their information security programs
  - To support Critical Infrastructure Protection (CIP) Planning
  - To facilitate exchange of effective security practices within the (federal) community

https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance

TPRM Maturity Model, NIST PRISMA

- NIST PRISMA identifies 5 Levels of program maturity
  1. Policies
  2. Procedures
  3. Implementation
  4. Testing
  5. Integration



https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7358.pdf

TPRM Maturity Model, Policies

- Characteristics
    - Program inception phase → "We need a TPRM program!"
    - Largely Governance driven
    - Creation of high level policies and procedures documents around generic "TPRM"
    - Little to no risk and remediation tracking
    - Little to no risk reporting visibility

TPRM Maturity Model, Procedures

- Characteristics
  - Assessments structured against a controls framework
  - Vendor self-assessment of controls
  - “One size fits all” assessment approach
  - Technical assessments on the rise
  - Procedures
    - Formalized, up to date
      - How/Where/Why procedures are to be performed
      - Defined responsibilities for involved players (BROs, IT, Procurement, etc.)
  - Some risk and remediation tracking
  - Limited visibility for risk reporting

TPRM Maturity Model, Implementation

- Characteristics
  - Vendor Tiering and Scorecards established
  - Risk-based levels of assessment and due diligence are performed
  - Enhanced risk and remediation tracking
  - Enhanced visibility for reporting
  - TPRM Global awareness is on the rise
  - Vendor Recertifications for high risk vendors

TPRM Maturity Model, Testing

- Characteristics
  - Assessments are tailored appropriately for the level of due diligence required
  - Issue tracking, remediation, validation is pushed to BROs
  - TPRM QA in place to ensure that all policies, procedures, and controls are acting as intended and that they ensure the appropriate information security level
  - Vendor Recertifications are more in-depth and more routine
    - Vendor completed self assessments face even more scrutiny (more knowledge of environment)
    - Inspection/validation of clean Penetration & Vulnerability Testing on a regular basis
    - Recertifications required for a broader range of vendors (determined by risk)

TPRM Maturity Model, Integration

- Characteristics
  - Security information gleaned from vendor assessments and recertifications is “weaponized” into proactive inquiry applied to all vendors of the same type that may be exposed to the same vulnerabilities and threats.
    - Example: Meltdown and Spectre vulnerabilities for Intel, AMD, and ARM processors
    - Example: Feb 2017 Google “broke” SHA-1 encryption rendering it obsolete)
  - Risk based assessment strategy is documented and effectively implemented
  - The frequency and rigor with which individual controls are tested depend on the risks that will be posed if the controls are not operating effectively
  - Risk and remediation tracking is well implemented
  - Highly visible reporting (Sr. Level Mgmt) often in the form of PMIs (Performance Metric Indicators)

TPRM Maturity Model, Integration

- Characteristics
  - Global Integration of TPRM
  - Automation of the TPRM process (Archer, Keylight)
  - TPRM process on Intelligent systems
  - Focused and high visibility reporting
  - Timely risk remediation
  - Policies, procedures, implementations, and tests are continually reviewed and improvements are made

Auditing TPRM Programs

- Top Level Goal - “The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.” – IPFF Standards
- IPFF 2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization’s governance, operations, and information systems regarding the:
  - Achievement of the organization’s strategic objectives.
  - Reliability and integrity of financial and operational information.
  - Effectiveness and efficiency of operations and programs.
  - Safeguarding of assets.
  - Compliance with laws, regulations, policies, procedures, and contracts

Auditing TPRM Programs, Scoping

- Recommendation: Take a “functional approach” to auditing TPRM programs and divide and conquer.
- Audit scoping and plan should be in-line with program maturity, otherwise findings and recommendations will not add a lot of value for Management
- TPRM Program maturity audit is a good place to start!

Auditing TPRM Programs, Functional Approach

Functional Area	Sub-Processes to Review
Governance	• Oversight • Vendor Lifecycle Management • Policies and Procedures • Risk Governance & Acceptance
Risk Assessment Process	• Risk Identification • Vendor Tiering/Classification • Controls evaluation • Due Diligence

Auditing TPRM Programs, Functional Approach

Functional Area	Sub-Processes to Review
Risk Documentation, Reporting, Remediation, and Monitoring	• Documentation & Reporting quality • Remediation process & timeliness • Contract Management • Security Rider reviews • SLA tracking and enforcement • Review of Risk Registry for accuracy, completeness, timeliness, etc.

Auditing TPRM Programs, Example

Function	Sub-process Detail
Program Governance - Oversight	❑ Determine if the level of oversight is appropriate ❑ Determine if the TPRM program aligns with organizational risk governance guidance ❑ Is there adequate resourcing for timely assessments? ❑ Level of TPRM integration with business/procurement functions ❑ Policies and Procedures ❑Current & Approved?

Auditing TPRM Programs, Example

Function	Sub-process Detail
Program Governance – Contract Compliance	Sample and perform a contract review for a population of vendors: ❑ Security & Privacy requirements in place? ❑ Breach notification in place? ❑ Cyber Insurance? ❑ Open remediation items? ❑ Business Continuity requirements ❑ Is the contract current?

Auditing TPRM Programs, Example

Function	Sub-process Detail
Program Governance – Vendor Lifecycle Management Considerations	For a sample of vendors, determine ❑ Assessment aging – overdue risks? ❑ Has the vendor ever been recertified? ❑ Are vendor contacts up to date? ❑ Determine if the Vendor Scorecard and Tiering is reasonable ❑ Vendor terminated procedures reasonable (data destruction)

Questions & Feedback

Thank you!

Zachary Couasnon is a Manager for RiSK Opportunities, Inc. currently advising and assisting clients with PCI, ISO, SOX, and Third Party Risk Management compliance. His experience includes over 11 years in the professional services space comprised largely of IT Audit and IT GRC related disciplines. Before joining RiSK, Zachary was an Internal Audit Manager for a multi-national electronics manufacturing company. Zachary is also a PwC and Deloitte & Touche LLP alum.

Zach.Couasnon@riskopportunities.com

Business & IT Advisory
Processes & Controls
Governance & Risk
Internal Audit
Compliance

RiSK
Opportunities