

Accenture Security

ACCENTURE SECURITY

DEMYSTIFYING THIRD PARTY RISK
MANAGEMENT (TPRM)

Sheldon Nailer, CISSP, CISA

Accenture Latvia, Security Team Lead

October 09, 2018

AGENDA

Background and Context

- Regulatory Landscape
- Cost of Failure
- Third-Party Risk Management Definitions

Third Party Risk Management Framework

TPRM Program Challenges and Critical Success Factors

Appendix



BACKGROUND AND CONTEXT

REGULATORY LANDSCAPE

Regulators are clear that organizations are responsible for services provided by third-parties as if it were provided in-house.

EU regulation

EU General Data Protection Regulation (GDPR):

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)”.

REGULATION (EU) 2016/679 Article 5
- Principles relating to processing of personal data

The EU (GDPR) makes organizations (“Controller/s”) **accountable** for data breaches caused by third-party service providers

US regulation

US (Federal Deposit Insurance Corporation) FDIC:

“An institution’s board of directors and senior management are ultimately **responsible for managing activities conducted through third-party** relationships, and identifying and controlling the risks arising from such relationships”

FIL 44-2008

US DODD-FRANK ACT:

“A service provider is “any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service”; a covered person is “any person that engages in offering or providing a consumer financial product or service; and any affiliate of a person described [as such] if such affiliate acts as a service provider to such person”

Dodd-Frank Act (Section 1002(26))

US Consumer Financial Protection Bureau (CFPB):

“[We] expect institutions to oversee business relationships with service providers with the **same level of scrutiny as any other line of business** in which it is engaged.”

CFPB 2012-03

US Office of the Controller of the Currency (OCC)

“ [A] third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise”. A bank’s **use of a third party “does not diminish the responsibility** of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws”.

OCC 2013-29

COST OF FAILURE CAN BE HIGH

Effective 3rd party management helps guard against incidents that can cause major financial and reputational damage to an organisation



FCA fines RBS, NatWest and Ulster Bank Ltd £42 million for IT failures

“The Financial Conduct Authority (FCA) fined the Royal Bank of Scotland Plc, (“RBS”) National Westminster Bank Plc (“NatWest”) and Ulster Bank Ltd (“Ulster Bank”) (the “Banks”) £42 million for IT failures which occurred in June 2012 and meant that the Banks’ customers could not access banking services. The actual cause of the IT incident was a software compatibility problem with the underlying cause being the Banks’ failure to put in place adequate systems and controls to identify and manage their exposure to IT risks” (FCA, Nov 2014)



Thomas Cook boss apologises to family over Corfu deaths

“The chief executive of Thomas Cook has apologised to the family of two children killed by carbon monoxide poisoning in Corfu after a public outcry over the company’s handling of the incident. Thousands of people have posted abuse on Thomas Cook’s Facebook page and threatened a boycott after the parents of Bobby and Christi Shepherd, who died aged six and seven, accused the company of “profiting” from the deaths when it emerged that Thomas Cook had received £3m of compensation from the hotel chain responsible for the incident” (FT, May 2015)



Universal Music Group

“It came to light that a Universal Music Group contractor neglected to protect an Apache Airflow server, leaving data exposed; while a Honda affiliate in India left two Amazon S3 buckets misconfigured for more than a year. The Honda mistake affects 50,000 users of the Honda Connect App, while UMG exposed corporate keys to the kingdom”. (Threatpost, June 2018)



2013 Target Data Breach

“Target’s profit for the holiday shopping period fell 46 percent from the same quarter the year before... It’s spokeswoman, Molly Snyder, says the intruders had gained access to the system by using stolen credentials from a third-party vendor.... the vendor was a refrigeration and heating company near Pittsburgh called Fazio Mechanical Services. A statement on Fazio’s website says its IT systems and security measures are in compliance with industry practices, and its data connection to Target was purely for billing, contract submission, and project management.” (Bloomberg, 2014)

TPRM DEFINITIONS

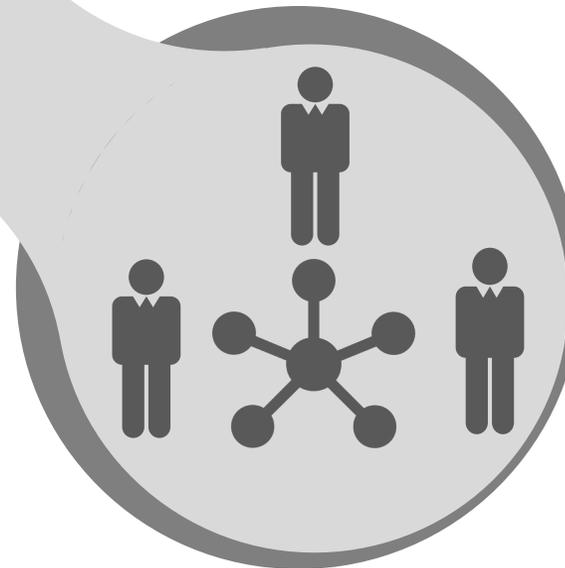
Third Parties

Any business arrangement between an organization and another entity, by contract or otherwise. Many people equate Third Parties with typical vendors, but that's not always the case.



Third Party Risk Management

The function responsible for identifying, managing and monitoring risks associated with Third Parties and providing competent oversight of these relationships. This enables the identification and engagement of Third Party service providers who can meet the needs of an organization based on requirements set forth in their contracts.



Third Party Risk Stratification

The process of rating and ranking the services provided to an organization by Third Parties based on risks inherent to the services (Operational, Strategic, Compliance, Credit, Reputational, etc.).

Third Party Relationship and Risk Management (TPRRM) is the oversight and governance of potential risk that arises from organizations relying upon outside parties to perform services on their behalf.

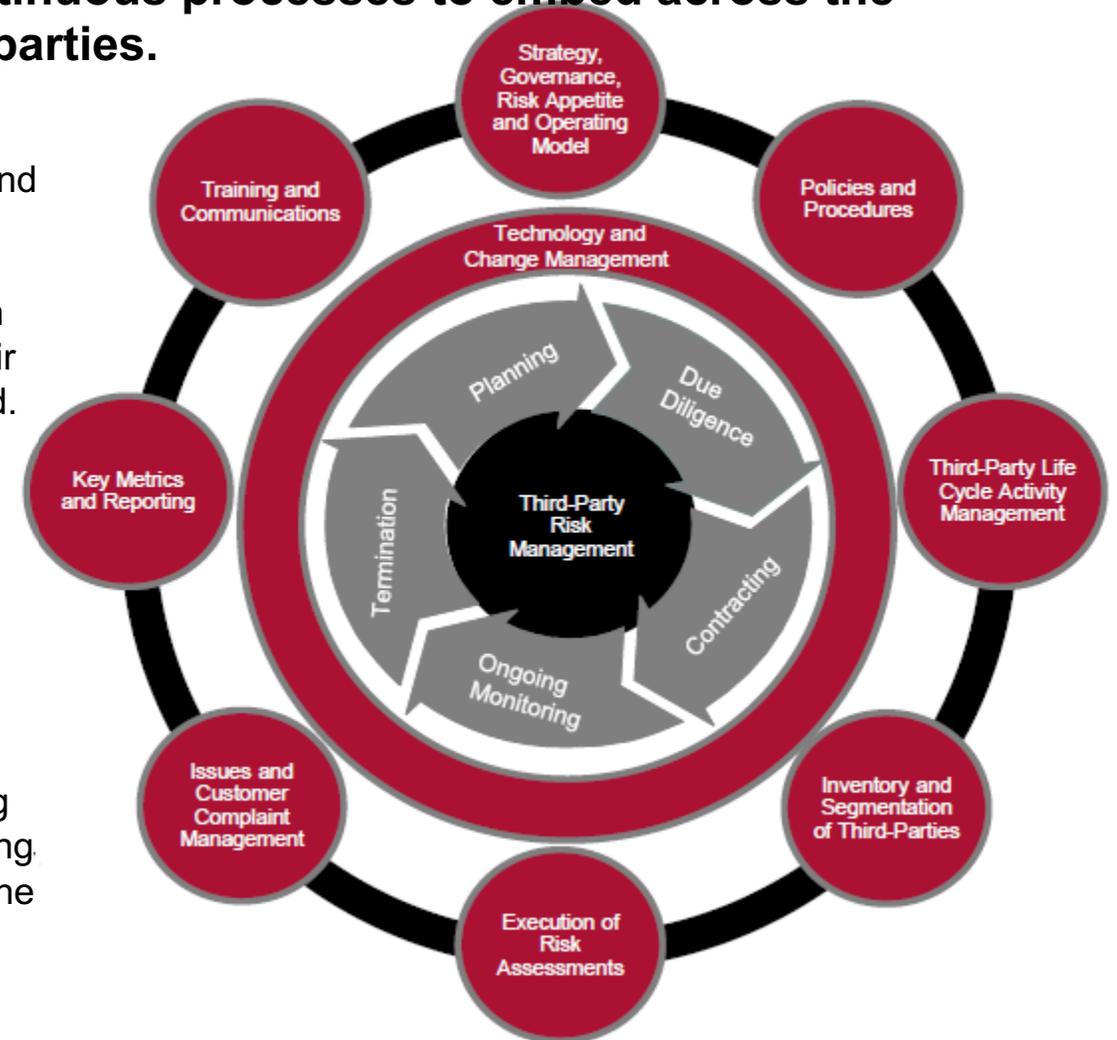
THIRD PARTY RISK MANAGEMENT FRAMEWORK

TPRM FRAMEWORK

A TPRM Framework outlines the key approach and continuous processes to embed across the organization to ensure appropriate control for all third-parties.

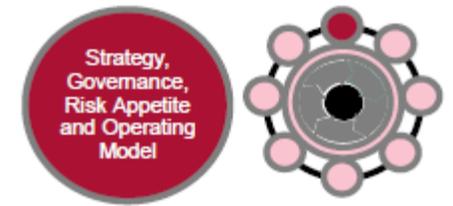
To be best in class, firms should develop or improve:

- **A comprehensive database of third-party relationships.** Many firms find it difficult to build this list; enterprise-wide surveys and data analytics are effective tools.
- **A comprehensive catalog of specific risks to which third-parties can expose the firm.** Many institutions don't fully understand all the risks their third-parties run. An 'intelligent' master risk register is useful in this regard.
- **A risk-based segmentation of third-parties.** Not all suppliers carry the same amount of risk. Firms need to better triage their suppliers to make sure the most effort is devoted to the highest risks.
- **Rules-based due diligence testing.** Carefully designed rules can help firms focus and prioritize their investigation of suppliers.
- **A disciplined governance and escalation framework.** At many firms, third-party risk management does not have a natural owner. Establishing one and giving that group the right decision-making powers is essential.
- **Integrated technology and MIS workflow process and tools.** Adapting current risk IT applications to third-party management is tricky, and building a new one is even harder. Off-the-shelf applications exist, but these run the risk of feeling like 'add-ons' and suffer with adoption. There must also be effective executive transparency to risk through dashboards and MI.

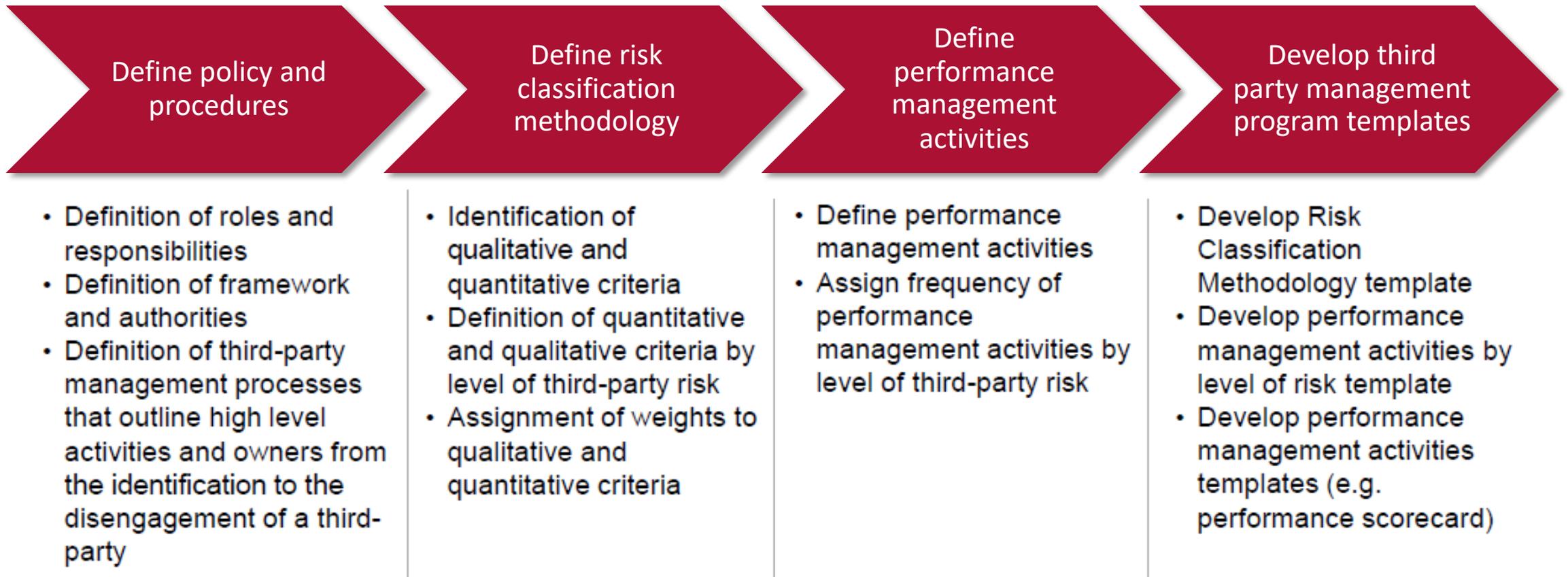


TPRM FRAMEWORK

TPRM PROGRAM APPROACH

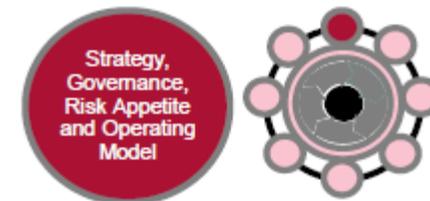


The Third-Party Management Program establishes a framework to manage third-parties within an organization. The establishment of the framework includes the definition of policies, procedures, methodology and templates to support the management of third-parties appropriate to the services and/or goods provided and associated level of risk.



TPRM FRAMEWORK

TPRM PROGRAM APPROACH



Examples of Third-Parties

| | |
|---|---|
|  IFAs |  Banks / Financial services |
|  National regulators |  Auto Finance / Loan / Dealerships |
|  Regional regulators |  Correspondent banks |
|  Intra group / IGRs |  Brokers & Investors |
|  White label resellers |  Business partners |
|  Professional memberships |  Charities / Philanthropic donations |
|  Property lease agreements / Landlords |  Debt buyers |
|  Financial Market Utilities |  Fund houses |
|  Trade bodies |  Advisors |
|  Tenants |  Agent/Network Management |
|  Vendors |  Audit / Tax services |
|  Sponsorship / Charities | |
|  Subscriptions | |
|  Educational institutions | |
|  Sub-Contractors | |
|  Utilities | |

Risks to consider

Typically considered risks

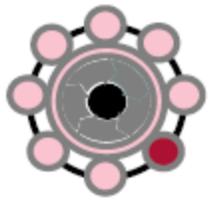
- Business Continuity & Resiliency
- Information Security
- Privacy
- Physical Security
- Reputational Risk
- Subcontractor Risk
- Financial Risk

Less frequently considered risks:

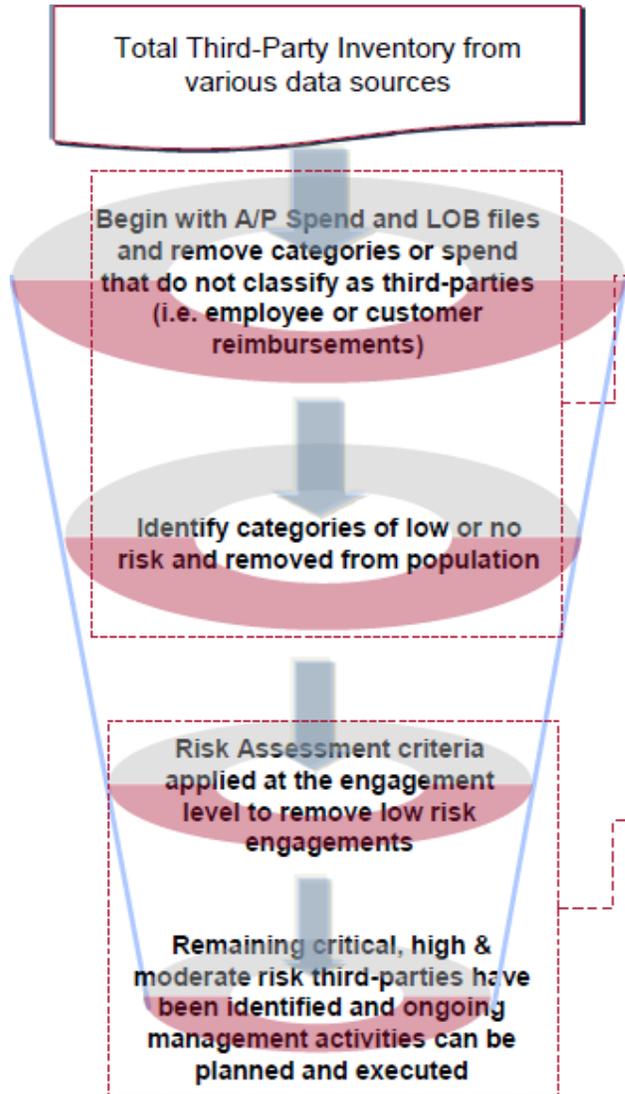
- Dependency Risk
- Legal & Regulatory Compliance
- Intellectual Property
- Commercial & Competition
- Operational Competency Risk
- Geographical Risk
- Contractual
- Sustainability
- Security & Data Protection
- Software Licencing
- Currency risk
- Concentration Risk
- Technology Risk

TPRM FRAMEWORK

ESTABLISHING THIRD-PARTY INVENTORY



Segmentation is a key element of TPRM, and results in appropriate resource alignment to Third-Party engagements



Common Third party Inventory data attributes

- Third-Party Name
- Third-Party Parent Name/Associated Third-Parties
- Product/ Service
- Third-Party Type (Business Process Outsourcing, Partnership, Technology etc.)
- Spend
- Business Lines/Processes Supported by the Third-Party
- Country/Region where Third-Party is based
- Contract Date (Engagement Date)
- Results of Third-Party Risk Classification
- Results of Third-Party Risk Assessments (e.g. Third-Party Information Security Assessments)

Third-Party Risk Classification Methodology

- The degree to which an organization is exposed if a third-party fails to meet the contractual commitments varies widely.
- A Third-Party Risk Classification Methodology allows an organization, through a series of pre-defined criteria, to identify the level of risk associated to a third-party (e.g. high, moderate, low, minimal to no risk).
- Risk classification of a third-party can include quantitative (e.g. spend, volume) and qualitative (e.g. number of third-parties that provide the same service, supports regulatory required activity) criteria.
- Qualitative and quantitative criteria can be assigned weights to emphasize key criteria within the organization (e.g. supports regulatory required activity higher weight than # of third-parties that provide the same service).
- Level of risk associated to a third-party can be used to determine Third-Party Management Program activities such as performance management and third-party operational reviews.

TPRM PROGRAM CHALLENGES AND CRITICAL SUCCESS FACTORS

TPRM PROGRAM CHALLENGES AND CRITICAL SUCCESS FACTORS

| | Challenge | Description | Critical Success Factors |
|---|---|--|--|
| 1 | Comprehensive database of third-parties | Many organisations find it difficult to establish this view; enterprise-wide surveys and data analytics are effective tools. | <ul style="list-style-type: none"> • Standard definition of a third-party • Exhaustive process to identify all third-parties • Single source of third-party data • Maintenance of third-party data |
| 2 | Comprehensive catalogue of third-party risks | Many organisations do not fully understand all the risk areas impacting their third-parties. An 'intelligent' master risk register is useful in this regard. | <ul style="list-style-type: none"> • Defining and implementing risk register • Capturing emerging risks • Risk register and controls library should map |
| 3 | Risk-based segmentation of third-parties | Organisations need to better triage their third-parties to ensure effort is applied to the right third-parties at the right time. | <ul style="list-style-type: none"> • Single risk segmentation model • Defined risk appetite • Risk management activities based on risk profile • Risk aggregation rules |
| 4 | Rules-based due diligence testing and ongoing monitoring | Carefully designed rules can help organisations focus and prioritise their investigation of third-parties. | <ul style="list-style-type: none"> • Systematic methodology for due diligence • Define rules for due diligence requirements • Scalable platform for execution & automation • Data into single source |
| 5 | Governance and escalation framework | TPRM does not always have a natural owner. Establishing one with the right decision-making powers is essential. | <ul style="list-style-type: none"> • Ownership agreed by all stakeholders • Owner to have sufficient influence over Third-Party Risk Management assets |
| 6 | Integrated technology and MIS | Off-the-shelf applications exist, but these run the risk of feeling like 'add-ons' and suffer with adoption. | <ul style="list-style-type: none"> • Defined and embedded processes • Holistic data model (third-parties) • Fit-for-purpose technology • Strong change control process for technology |

THANK YOU!

ACCENTURE LATVIA SECURITY PRACTICE

DATA PRIVACY & GDPR · SECURITY RISK ASSESSMENTS SECURITY · ADVISORY SERVICES

CYBER SECURITY TESTING · VULNERABILITY MANAGEMENT

ISO 27001 · SPLUNK · CyberArk

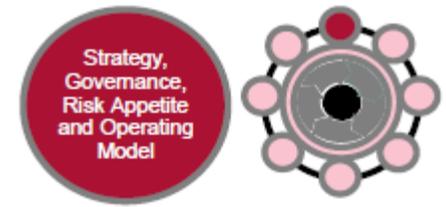


CONTACTS: sheldon_nailer@hotmail.com

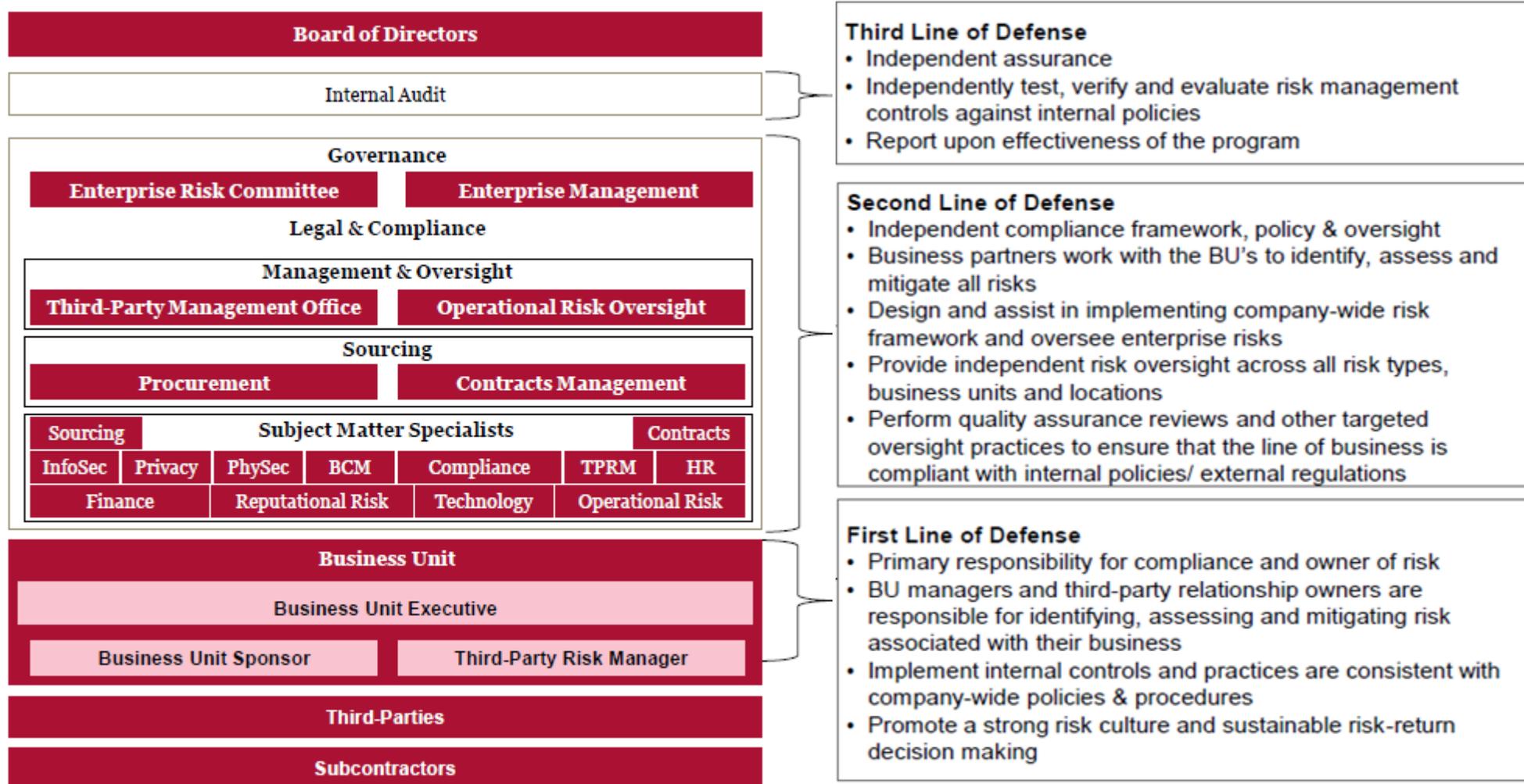
APPENDIX

TPRM FRAMEWORK

TPRM GOVERNANCE FRAMEWORK



A specific TPRM function can be embedded within the existing governance framework, providing appropriate internal expertise. A TPRM strategy is supported by three lines of defense –the first line lies within each individual Line of Business and is empowered by the second line who owns the provision of ongoing guidance, tool support, and facilitation of cross-business collaboration. The third line is responsible for evaluating the design and operating effectiveness of the Program.



TPRM FRAMEWORK

BUILDING ROBUST THIRD-PARTY RISK MANAGEMENT POLICIES

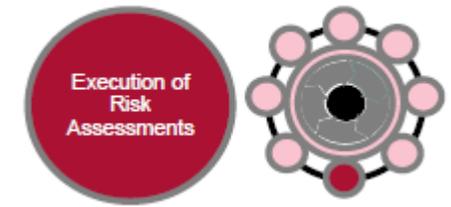


Policies and procedures for Third-Party Risk Management should at a minimum consider and include:

- **Compliance and Regulation:** Appropriate oversight of third-parties to ensure they comply with legal requirements, any supervisory guidance, and internal policies and procedures
- **Due Diligence.** Steps to perform appropriate due diligence on potential and current third-party qualifications, expertise, capacity, reputation, complaints, information security, document custody practices, business continuity, and financial viability
- **Business Continuity:** Processes to prepare contingency and business continuity plans that ensure the continuing availability of critical third-party services and business continuity of the organization both to address short-term and long-term service disruptions and to ensure an orderly transition to new service providers should that become necessary
- **Information Security:** Measures to ensure all original records transferred to third-parties remain within the custody and control of the third-party and are returned to designated custodians at the conclusion of the performed service, along with all other documents necessary for the organization's files
- **Contracts:** Processes to ensure that third-party contracts provide for adequate oversight, including requiring third-parties adherence to the organization's standards, measures to enforce third-party contractual obligations, and processes to ensure timely action with respect to third-party performance failures
- **Fee Structures:** A review of fee structures for third-parties to ensure that the method of compensation considers the accuracy, completeness, and legal compliance of activities and is not based solely on volumes or meeting processing timelines
- **Deliverables:** Processes to ensure periodic reviews of third-party's work for timeliness, competence, completeness, and compliance with all applicable Legal Requirements, and the organization's contractual obligations to investors
- **Customer Complaints:** Processes to review customer complaints about third-party's services
- **Certifications:** A periodic certification process for firms that were qualified/designated to serve as third-parties to the organization and to ensure they continue to have the experience and competence required to perform the services
- **Accuracy:** Measures to ensure the accuracy of all documents filed or otherwise utilized on behalf of the organization

TPRM FRAMEWORK

EXECUTION OF RISK ASSESSMENT



Execution of risk assessment requires understanding the scope, identifying gaps, developing risk mitigation enhancements, tracking status towards target state. Assessment and heat map tools can aid significantly in the execution of risk assessment

Third-Party Risk Assessment

| Risk Assessment | Scope | Status | | Status |
|---------------------------|----------------------------------|--------------|----------------|-------------|
| | | Gap Analysis | Remediation | |
| Information Security Risk | TPISA | ● | ● | In Progress |
| | Vulnerability Assessment | ● | ● | |
| | SOC1/SOC2 | ● | ● | |
| Compliance Risk | AML | ● | Not Applicable | |
| | Anti-Bribery (AB&C) | ● | Not Applicable | |
| | Sanctions Screening | ● | ● | |
| | Customer Compliant | ● | ● | |
| Operational Risk | CoB Testing | ● | ● | |
| | 4 th Party Assessment | ● | ● | |
| | Performance Review | ● | ● | |
| | Financial Assessment | ● | Not Applicable | |
| | Exit Strategy | ● | ● | |
| | Legal Hold | ● | ● | |

Third-Party Risk Heat Map

| | Third-Party | System Registration | Contract Analysis | Performance Review | Financial Evaluation | COB Testing | Exit Strategy | 4th Party Attestation | Information Security |
|------------------------------|------------------|---------------------|-------------------|--------------------|----------------------|-------------|---------------|-----------------------|----------------------|
| Critical (Externally Hosted) | Third-Party Name | C | O | C | C | E | C | C | C |
| | Third-Party Name | C | E | C | C | E | C | C | C |
| | Third-Party Name | C | O | C | C | E | C | C | C |
| | Third-Party Name | C | O | C | C | E | C | C | E |
| Critical (Internally Hosted) | Third-Party Name | C | O | E | C | | | | |
| | Third-Party Name | C | E | C | C | | | | |
| Major Spend | Third-Party Name | C | O | C | C | | | C | TBD |
| | Third-Party Name | C | O | C | O | | | C | |
| | Third-Party Name | C | O | C | C | | | C | |
| | Third-Party Name | C | O | C | C | | | C | |
| | Third-Party Name | C | O | C | C | | | C | |

C = Complete O = On Track / In progress E = Exception / Gaps Identified

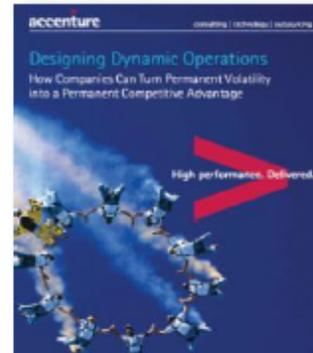
ACCENTURE'S TPRM THOUGHT LEADERSHIP

Accenture's TPRM capabilities are supported by a significant number of 'ready to go' pieces of research that bring insight and will accelerate the approach to the engagement.

Procurement Risk Management



Designing Dynamic Operations



Supplier Relationships: Cracking the Value Code



Supplier Working Relationship Index



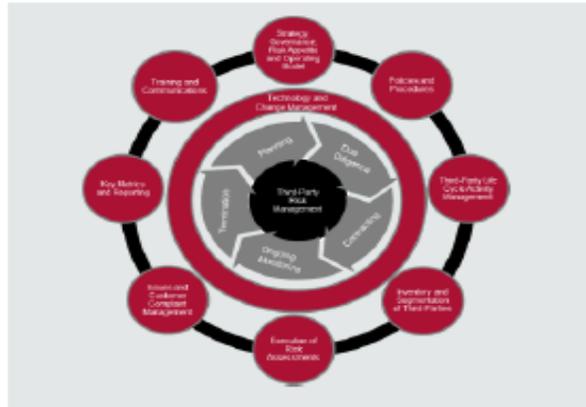
TPRM Benchmarking Study

| Questions | Client Bank | Large US Bank 1 | Large US Bank 2 | Large US Bank 3 |
|--|----------------------------|---------------------|----------------------------|----------------------------|
| <i>Contracted Procurement & Vendor Management Functions: Which other management functions are contracted for the Bank?</i> | | | | |
| Procuring? | Centralized | Centralized | Modular centralized | Decentralized based on LOB |
| Vendor Risk Mgmt? | Modular centralized | Modular centralized | Modular centralized | Modular centralized |
| Vendor Ops Mgmt | Decentralized based on LOB | Modular centralized | Decentralized based on LOB | Modular centralized |
| Site Mgmt? | Decentralized based on LOB | Centralized | Modular centralized | Modular centralized |
| Vendor Performance Mgmt? | Decentralized based on LOB | Modular centralized | Decentralized based on LOB | Modular centralized |
| Legal/IC contracting? | Centralized | Centralized | Modular centralized | Decentralized based on LOB |
| Human Resources? | Centralized | Centralized | Centralized | Decentralized based on LOB |
| <i>Governance & Oversight: Does a Steering Committee (SC) oversee vendor engagement for deal approval and resolution / vendor strategy definition?</i> | | | | |
| Does an SC exist? | X | X | X | X |
| Is Banking implemented? | X | X | ✓ | ✓ |
| Is Vendor Risk Mgmt implemented? | X | X | ✓ | ✓ |
| Is Vendor Ops Mgmt implemented? | X | X | ✓ | ✓ |
| Is Site Mgmt implemented? | X | X | ✓ | ✓ |
| Is Vendor Perf. Mgmt implemented? | X | X | ✓ | ✓ |
| Is Legal/IC contracting implemented? | X | X | ✓ | X |
| Is HR implemented? | X | X | X | X |
| Is any other implemented? | X | X | Comp Risk & Compliance | X |

ACCENTURE TPRM TOOLS

Accenture's TPRM are supported by a significant number of 'ready to go' tools and assets that bring insight and will accelerate delivery of the TPRM assessment, future state definition, and reporting templates.

TPRM Capability Framework



Requirements Template

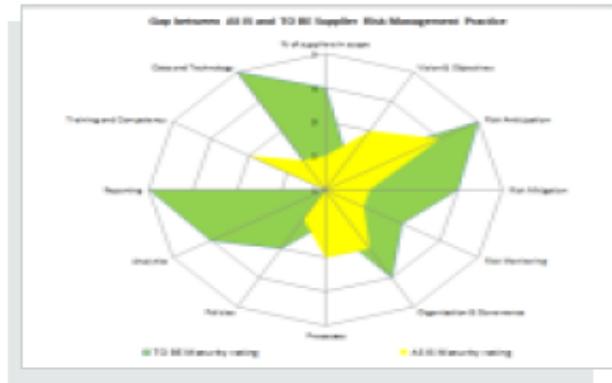
| High Level Standards | Description | Impact on Sourcing? |
|---|--|---------------------|
| Principles for Businesses | the fundamental obligations of all firms under the regulatory system | ○ |
| Senior Management Arrangements, Systems and Controls | the responsibilities of directors and senior management | ● |
| Threshold Conditions | the minimum standards for becoming and remaining authorised | ○ |
| Statements of Principle and Code of Practice for Approved Persons | the fundamental obligations of approved persons | ○ |
| The Fit and Proper test for Approved Persons | the minimum standards for becoming and remaining an approved person | ○ |
| Financial Stability and Market Confidence Sourcebook | Provisions relating to financial stability, market confidence and short selling | ○ |
| Training and Competence | the commitments and requirements concerning staff competence | ○ |
| General Provisions | interpreting the Handbook, fees, approval by the FSA, emergencies, status disclosure, the FSA logo and insurance against fines | ○ |
| Fees Manual | the fees provisions for funding the FSA, FOS and FSCS | ○ |

Legend on Sourcing:
 ○ None
 ● High - direct requirement for sourcing to comply
 ○ Medium - sourcing should consider to align with subson Great Coherence compliance

Regulation Analysis and Experience

| | |
|---|---|
| Bank Regulations - Basel 2.5: Market Risk, Trading Book, Remuneration, Poinc, Large Exposures, Securitization, Re Securitization, Disclosure Securitization Risk, Cross Border Supervision - Basel III: Hybrid Capital Instruments, Definition of Capital, Capital Requirements, Leverage Ratio, Liquidity Risk Management, Liquidity Standards, Countervailing Credit Risk (CCR), Countervailing Measures, Systemically Important Financial Institution (SIFI), Listing Walk, Single Rule Book - EMIR: Central Counterparty (CCP) - EBA: Stress Tests - Dodd Frank: E.g. Volcker Rule, Legal Entity Identifier (LEI), Central Counterparty (CCP), OTC, Swap Protocol Rule etc. | Capital Markets / Settlements / Collaterals / Payments - Constitution of Central Securities Depositories (CSDs) - Target 2 Securities (T2S) - Collateral Central Bank Management (CCBM2) - Single Euro Payments Area (SEPA) Migration - Regulation of the European Parliament and of the Council on short Selling and certain aspects of Credit Default Swaps - New Market Abuse Directive (MAD) - Securities Law Directive (SLD) |
| Taxation - European Financial Transaction Tax (FTT) - FATCA - Foreign Account Tax Compliance Act - Double Tax Agreements (DTA) - US Estate Tax | Data Protection / Anti-Corruption - Consumer Data Protection Regime for Belgium - UK Bribery Act 2010 |
| Investment Services Regulations - MiFID I + MiFID II / MiFIR - Markets in Financial Instruments Directive - UCITS III / IV - Undertaking for Collective Investment in Transferable Securities - ESMA - Consultation of Exchange-traded and Structured OIGAW-Funds - AIFMD - Alternative Investment Fund Managers Directive - Regulations on Credit Rating Agencies - Prospectus Directive | Accounting / Financial Reporting - IFRS 9 - Financial Instruments (Replacement of IAS 39) - IFRS 13 - Fair Value Measurement - IASB - The Committee of Sponsoring Organizations of the Treadway Commission |
| | German Regulations - Gesetz zur Optimierung der Geschäftsverteilung und zur Konsolidierung des Finanzanlagenbewertungs- und Vermögensverwaltungsrechts - MaRisk / ICAAP - Internal Capital Adequacy Assessment Process - Verordnung über den Ersatz von Mitarbeitern in der Anlageberatung als Inhabersauftrag und Compliance-Beauftrag (Pflichtentwurf) |

Maturity Diagnostic



Gap Analysis

| Area | Requirement | Current State | Target State | Gap | Impact | Priority |
|--------|---------------|---------------------|--------------|--------|--------|----------|
| Area 1 | Requirement 1 | Not Compliant | Compliant | High | High | High |
| Area 2 | Requirement 2 | Partially Compliant | Compliant | Medium | Medium | Medium |
| Area 3 | Requirement 3 | Compliant | Compliant | Low | Low | Low |

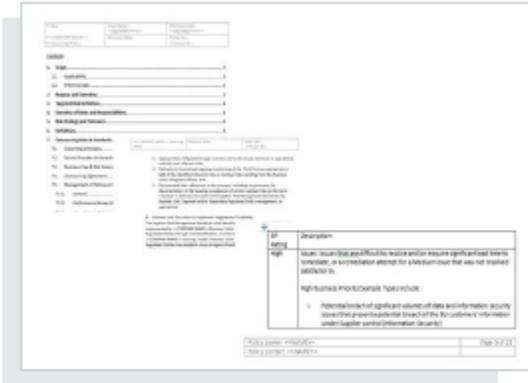
Target Operating Model



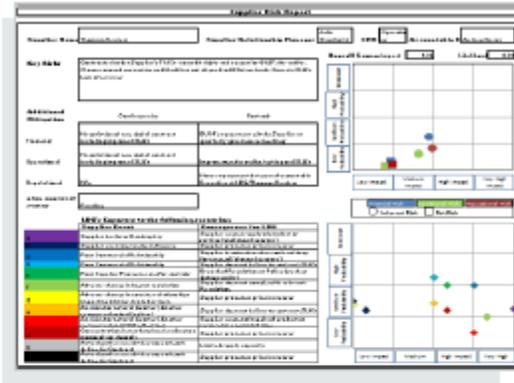
ACCENTURE TPRM TOOLS (CONTINUED)

Accenture's TPRM are supported by a significant number of 'ready to go' tools and assets that bring insight and will accelerate delivery of the TPRM assessment, future state definition, and reporting templates.

Model Policies and Governance



TPRM Toolkit



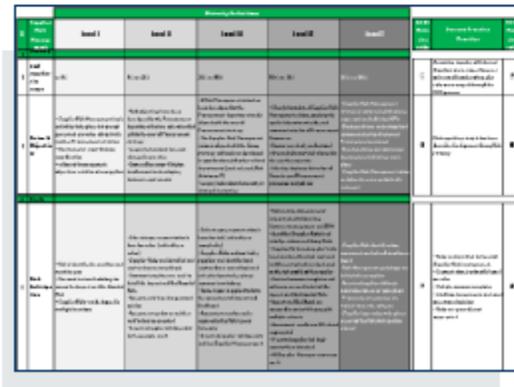
TP Monitoring Scorecard

| Vendor for evaluation | Accenture | Add New Vendor | Last Evaluation | Next Evaluation |
|---|---------------|----------------|-----------------|-----------------|
| Select a vendor for evaluation | Mid-Year 2022 | | | |
| Select a period for evaluation | | | | |
| A. Key Commercial Performance | | | | |
| Category | Metric | Score | Rating | |
| A.1. Service Performance | | | | |
| 1. On-time Delivery | 95% | 95% | High | |
| 2. Quality of Service | 90% | 90% | High | |
| 3. Customer Satisfaction | 85% | 85% | High | |
| 4. Incident Resolution | 80% | 80% | High | |
| 5. Compliance | 75% | 75% | High | |
| A.2. Business Performance | | | | |
| 6. Revenue Growth | 10% | 10% | High | |
| 7. Profitability | 15% | 15% | High | |
| 8. Market Share | 20% | 20% | High | |
| A.3. Risk/Compliance Performance | | | | |
| 9. Risk Rating | Low | Low | High | |
| 10. Compliance Score | 95% | 95% | High | |
| B. Operational Performance | | | | |
| 11. Efficiency | 90% | 90% | High | |
| 12. Reliability | 85% | 85% | High | |
| 13. Scalability | 80% | 80% | High | |
| 14. Flexibility | 75% | 75% | High | |
| 15. Innovation | 70% | 70% | High | |
| 16. Sustainability | 65% | 65% | High | |
| 17. Social Responsibility | 60% | 60% | High | |
| 18. Environmental Impact | 55% | 55% | High | |
| 19. Governance | 50% | 50% | High | |
| Summary | | | | |
| Overall Score: 85% | | | | |
| Risk Rating: Low | | | | |
| Compliance Score: 95% | | | | |
| Operational Performance: 80% | | | | |

TP Tiering Strategy

| Vendor Tier | Definition / Criteria | Implication for Vendor | Implication for client |
|-------------------|---|--|--|
| Strategic | <ul style="list-style-type: none"> Global, wide or multi-regional Critical to client performance or core business Highly visible to client Highly visible to client | <ul style="list-style-type: none"> Highly visible to client Highly visible to client Highly visible to client Highly visible to client | <ul style="list-style-type: none"> Highly visible to client Highly visible to client Highly visible to client Highly visible to client |
| Preferred | <ul style="list-style-type: none"> Global, wide or multi-regional Critical to client performance or core business Highly visible to client Highly visible to client | <ul style="list-style-type: none"> Highly visible to client Highly visible to client Highly visible to client Highly visible to client | <ul style="list-style-type: none"> Highly visible to client Highly visible to client Highly visible to client Highly visible to client |
| Approved | <ul style="list-style-type: none"> Global, wide or multi-regional Critical to client performance or core business Highly visible to client Highly visible to client | <ul style="list-style-type: none"> Highly visible to client Highly visible to client Highly visible to client Highly visible to client | <ul style="list-style-type: none"> Highly visible to client Highly visible to client Highly visible to client Highly visible to client |
| Restricted | <ul style="list-style-type: none"> Global, wide or multi-regional Critical to client performance or core business Highly visible to client Highly visible to client | <ul style="list-style-type: none"> Highly visible to client Highly visible to client Highly visible to client Highly visible to client | <ul style="list-style-type: none"> Highly visible to client Highly visible to client Highly visible to client Highly visible to client |

TP Diagnostic



TP Segmentation Tool

