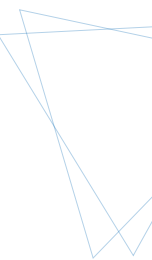# HCL
Third-party **Risk Management** Services

Driving business excellence in the evolving third-party risk.

Third-party Risk Management

In today's fast-growing usage of third parties in organizations, businesses worldwide are compelled to manage their vendor risks and compliance risk more diligently. With an increase in third-party-related incidents, organizations are finding themselves at the brunt of punitive action by both customers and regulatory bodies.

In view of this, organizations need to onboard a mature third-party risk management approach as opposed to the traditional approach where due diligence takes a backseat after the vendor is selected.

Per a global survey conducted in 2018 by (Deloitte, n.d.), the compliance risk posed by third parties has extended to new levels, exposing businesses worldwide to the threat of major business failures and

customer service disruption. The impact of changing regulations is one of the major contributing factors to the increased perception of inherent risks in third-party management.

Although investment in third-party risk management has been growing year-on-year globally, the results have not been satisfactory due to ineffective TPRM processes in place. Therefore, it is imperative for companies worldwide to incorporate a more mature third-party risk model to proactively identify, manage, and mitigate risks, and implement proper governance, risk, and compliance processes.

While many organizations monitor the performance of most of their suppliers effectively in terms of quality and timeliness, there are other suppliers who are rarely scrutinized based on their performance. This tunnel vision of organizations has exposed them to significant hidden risks in terms of data leaks, business disruption, and regulatory non-compliance.

Facts

Estimated direct source of security incidents from third-party vendors was 19% in 2017[1]

Organizations that are integrated or optimized in managing their third-party partnerships are now typically investing over $3 million annually on TPRM initiatives[2]

The investments made in EERM in 2017 will begin to pay dividends in either 2018 or 2019—in line with the respondents' realistic assessment that it takes two to three years for an organization of any size[3]

[1](PwC, 2018) The Global State of Information Security Survey
[2](Deloitte, 2018) Extended enterprise risk management survey 2018
[3](Deloitte, 2018) Extended enterprise risk management survey 2018

Critical challenges in third-party risk
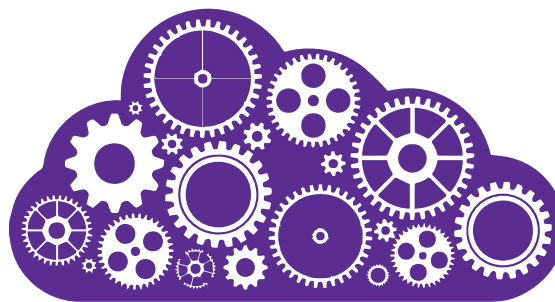
Regulatory

- Changes in the regulatory and compliance landscape
- Regulations at every corner: European GDPR, California CDPA, Singapore Cybersecurity Act, FTC, ISO, AML, Dodd Frank, and others
- Increasing compliance pressure

Governance

- Absence of dedicated personnel to risk-related management activities
- Lack of standardized third-party compliance process and escalation framework
- Siloed approach to tackle third-party risks rather than a holistic approach
- Lack of awareness of global industry standards and compliance training

Operational

- Absence of comprehensive third-party information inventory
- Increased complexity of third-party network in organizations
- Inconsistency of standards and procedures related to third-party risk management systems (TPRMS) in business units
- Absence of a systematic due diligence process
- Narrow focus on cost drivers instead of value drivers

Legal and Financial

- Regulatory breach and customer service disruption as top risks
- Huge penalties imposed on organizations due to non-compliance
- Reputational damage due to financial fraud
- Increased dependence on third parties have led to increased costs
- Risk of contract-related cost leakage in supplier engagements

Technology

- Disruptive technology, a key challenge to organization
- Evolving technology infrastructure and delivery models
- Execution gap faced in organizations due to inability of supporting tools and processes
- Low confidence in existing delivery and technology platforms for managing third parties
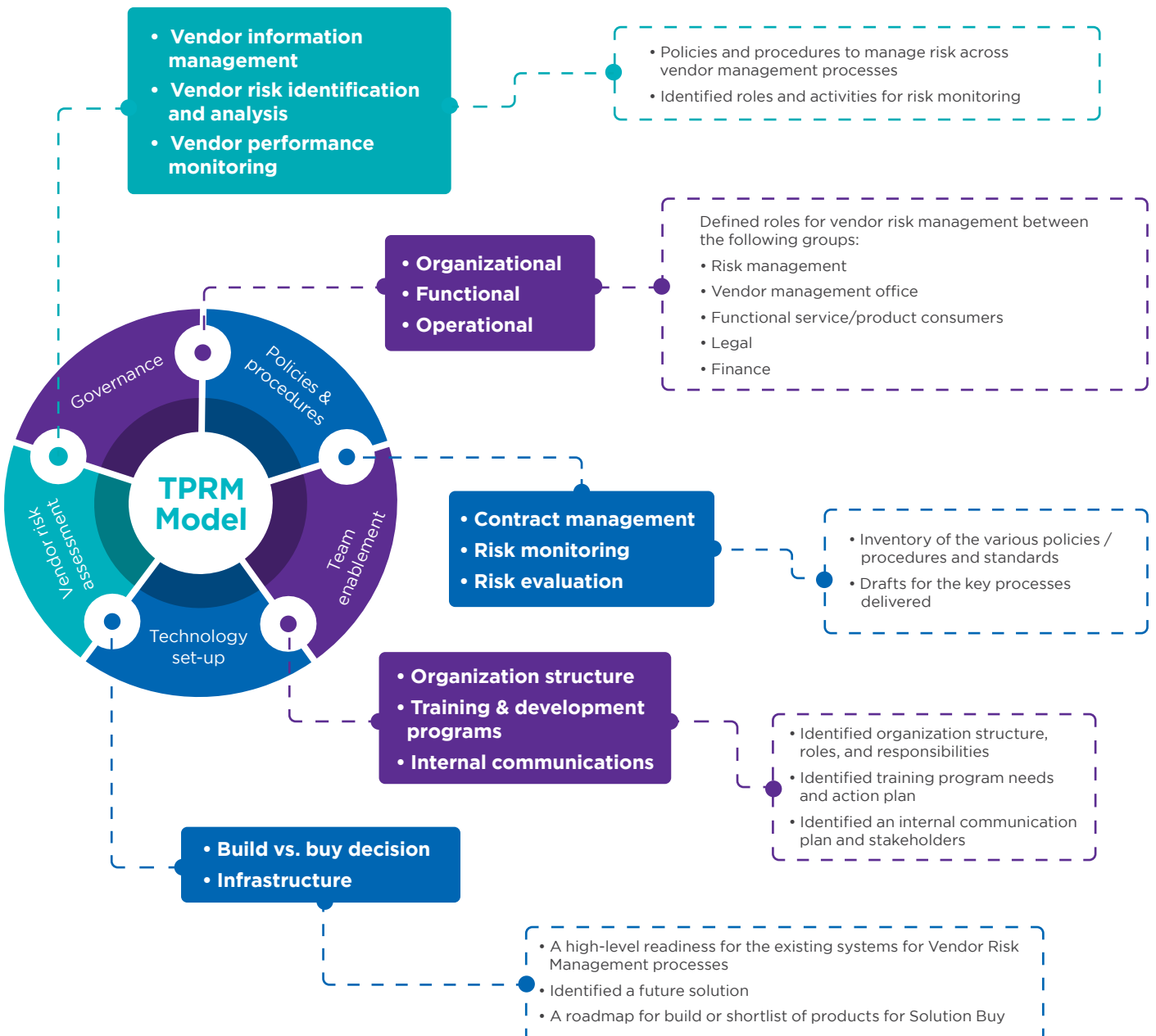
HCL Third Party Risk Management framework

> *HCL is a pioneer in the field of governance, risk, and compliance. With an established Center of Excellence for governance, risk, and compliance consulting, our seasoned and experienced practitioners provide strategic insights and advisory services to tackle risk and compliance challenges in the third-party risk landscape.*

Powered by its rich experience, the GRC team of HCL has established a well-defined TPRM model that helps organizations across various industry verticals seek timely vendor risk insights and respond to third-party risk exposures.

Bridging the gap between the suppliers and customers, the HCL TPRM model streamlines the entire risk management process. It focuses on conducting an effective vendor risk assessment, developing constructive collaboration between interested parties, integrating appropriate technology/tools to monitor third-party risks, and defining a set of policies to gain a centralized view of the entire third-party risk landscape.

Vendor information management
Vendor risk identification and analysis
Vendor performance monitoring

- Policies and procedures to manage risk across vendor management processes
- Identified roles and activities for risk monitoring

Organizational
Functional
Operational

Defined roles for vendor risk management between the following groups:
- Risk management
- Vendor management office
- Functional service/product consumers
- Legal
- Finance

TPRM Model

Governance
Policies & procedures
Team enablement
Technology set-up
Vendor risk assessment

Contract management
Risk monitoring
Risk evaluation

- Inventory of the various policies / procedures and standards
- Drafts for the key processes delivered

Organization structure
Training & development programs
Internal communications

- Identified organization structure, roles, and responsibilities
- Identified training program needs and action plan
- Identified an internal communication plan and stakeholders

Build vs. buy decision
Infrastructure

- A high-level readiness for the existing systems for Vendor Risk Management processes
- Identified a future solution
- A roadmap for build or shortlist of products for Solution Buy

Key service offerings of the HCL TPRM model

Monitoring and analysis

- Provide a clear picture of real-time risks by generating actionable management reports
- Integrate processes with new or existing technology platforms to track and monitor data

Due diligence

- Perform appropriate risk-based inspection through due diligence questionnaires
- Enable companies to assess third-party controls and foster a culture of accountability through systematic due diligence

Dashboard & reporting

- Reporting is done on the risks identified during vendor assessment and performance is monitored on graphical dashboards, a holistic approach tailored toward multiple levels of engagement

Monitoring & analysis — 01

Dashboard & reporting — 02

Risk assessment — 03

Program management — 04

Due diligence — 05

Key service offerings
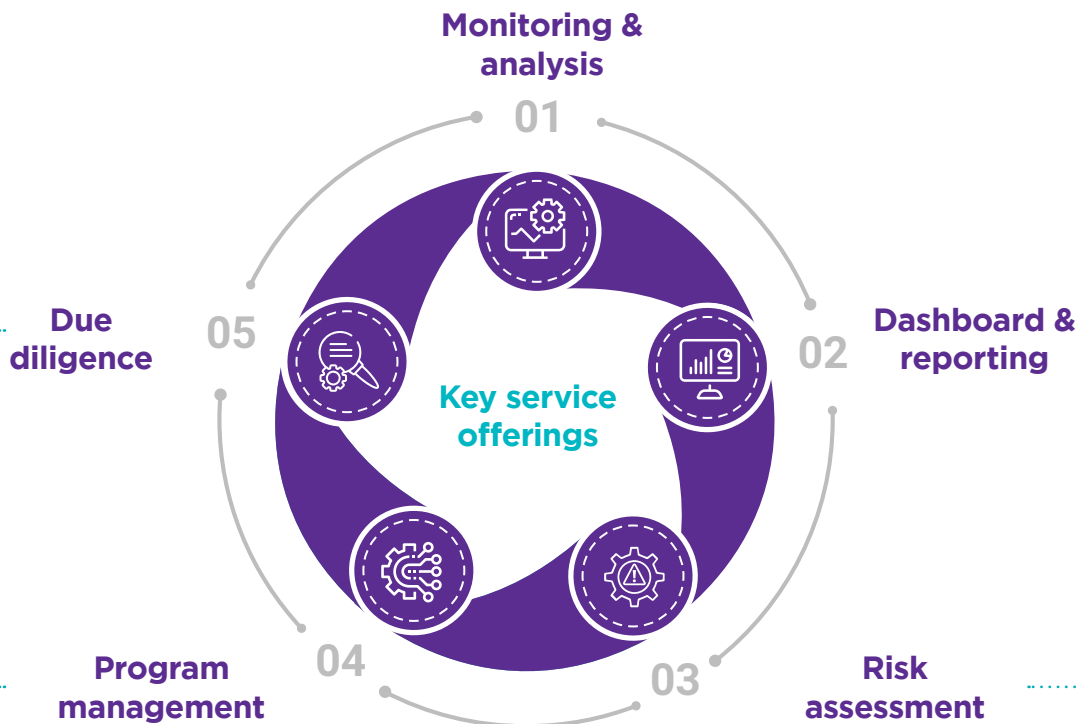
Program management

- Establishes an enhanced TPRM program for remediation tracking and remediation management
- Helps design appropriate training and awareness programs to orchestrate the company's internal function, supplier processes, and customer's relationship effectively

Risk assessment

- Includes a detailed risk assessment of the vendor environment against global standards
- Application Assessment
- Infrastructure Assessment
- Service Mgmt. Assessment
- Regulatory Risk Assessments
- Third-party Audits

TPRM as a Service

Automation on leading GRC and vendor risk management platforms

Centralizes vendor profile

Self-service portal for vendors and relationship managers
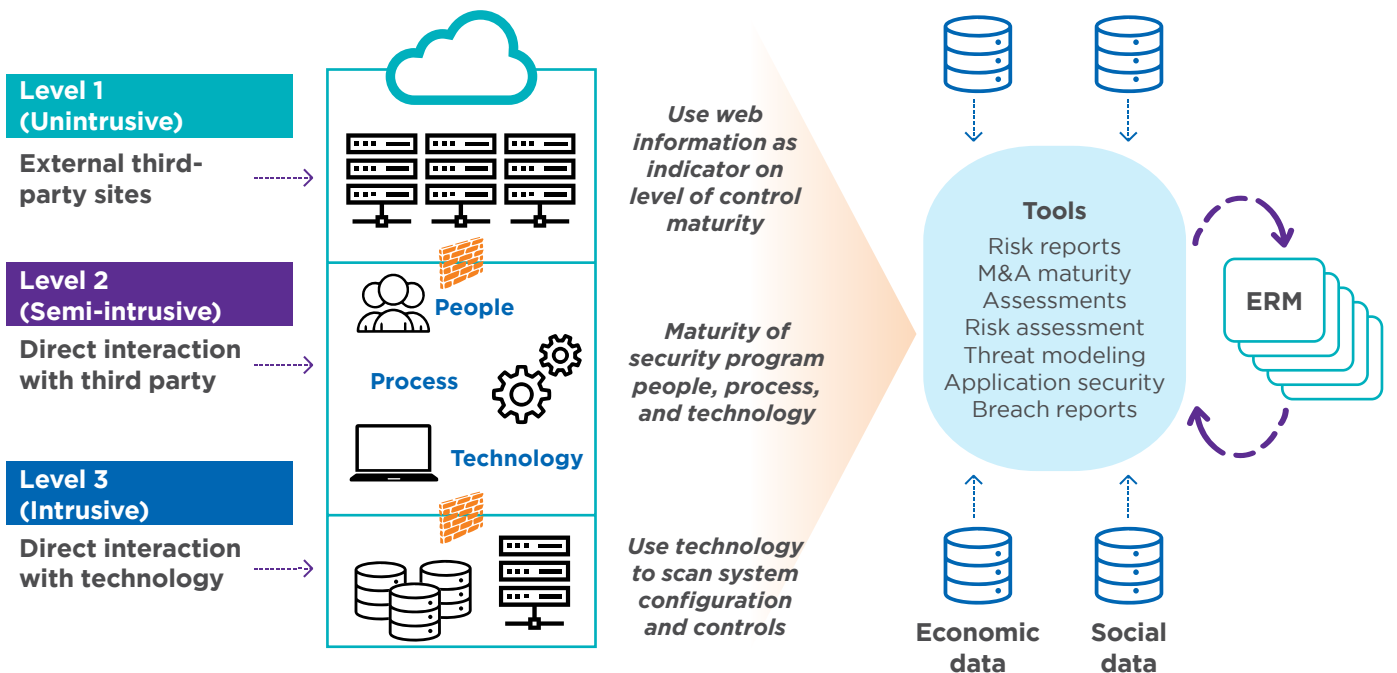
Analyses business impact

Automates measurement and control compliance

Monitors vendor management program end to end

Third-party risk monitoring

Level 1 (Unintrusive)

External third-party sites

Level 2 (Semi-intrusive)

Direct interaction with third party

Level 3 (Intrusive)

Direct interaction with technology

People

Process

Technology

Use web information as indicator on level of control maturity

Maturity of security program people, process, and technology

Use technology to scan system configuration and controls

Threat intelligence

Financial data

Tools
Risk reports
M&A maturity
Assessments
Risk assessment
Threat modeling
Application security
Breach reports

ERM

Economic data

Social data

Case studies of TPRM

Supplier risk assessment program for a leading US pharmaceutical company

The HCL GRC team implemented our third-party risk management model for a leading US pharmaceutical manufacturing company which had multiple vendors around the globe. More than 3,200 vendors spread across America, Europe, and South East Asia region were assessed. We assisted this company by conducting rigorous supplier risk assessments and helped them identify vulnerabilities in their security systems.

Benefits

Highly effective regulatory coverage of vendor risks against global standards

Establishment of proactive risk mitigation in the supply chain process

Third-party security and compliance assessment for a global bank

The customer is a leading global bank headquartered in Canada with over 1,700 vendors across America, Europe, and the APAC region. Siloed vendor management processes across various departments was the key challenge for the customer. The customer sought a common methodology for the bank's Integrated Risk Management (IRM) program to assess vendors. The HCL team implemented a supplier risk assessment program for our client that took into account baseline regulatory controls of vendors and centralized the facilitation of control testing.

Benefits

A transition from quality to compliance-centric operations

Better control of sourcing governance, risk management & vendor evaluation by converging multiple GRC activities

GRC platform enabled TPRM for a leading insurance organization

The customer is an insurance organization which started a Federal Reserve supervision program in its premise to oversee higher standards of corporate compliance. It sought to enhance technology towards vendor management across the organization and develop processes required to perform periodic regulatory reporting to the Federal Reserve. The HCL team suggested GRC platform implementation for risk and compliance management to mitigate core risks mostly arising out of supplier processes.

Benefits

Implementing integrated IT GRC third-party risk-related processes on a common platform through automation

A strategic roadmap for enterprise GRC aligned to the client's risk and compliance objectives in changing the regulatory landscape

A flexible and scalable environment platform to enable the business to deliver high performance through real-time reporting and dashboards

Higher customer trust and satisfaction

Consistent and systematic TPRM approach

Technology-enabled risk function

Key benefits of TPRM services

Holistic view of inherent risks

Sustainable business growth

Greater supplier delivery performance
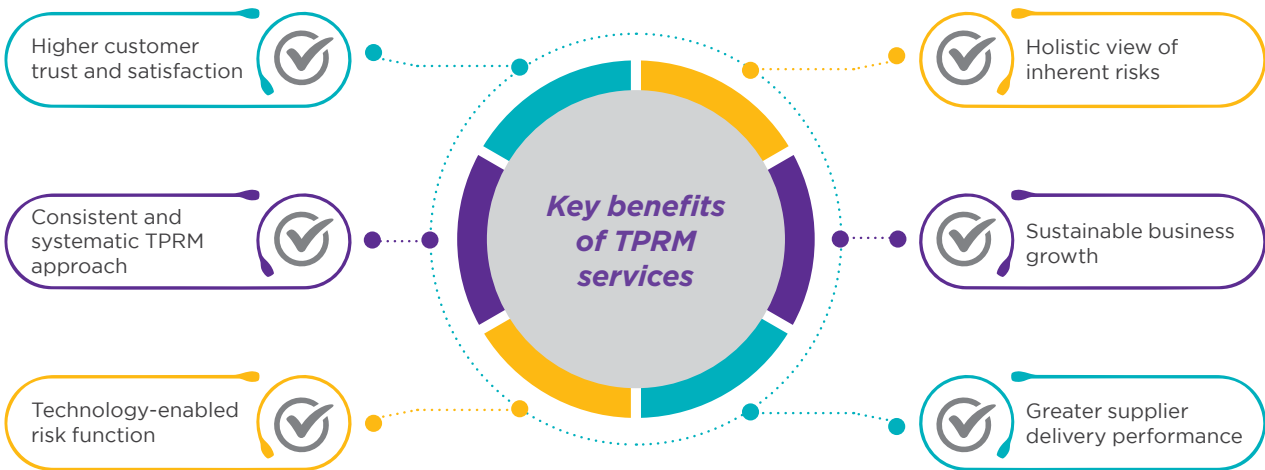
[Exhaustive coverage of global control standards: ISO 27001:2013, COBiT, COSO, ITIL, ISO 31000, CSA, eSCM, OCTAVE, ISO 22301, NIST,PCI-DSS, SOX, HIPPA, FFIEC, DoD, MAS, FISMA, DPA, PIPEDA, GDPR, etc]

Contact Us:

To find out more write to **Cybersecurity-GRC@hcl.com**
or visit: **https://www.hcltech.com/cyber-security-grc-services/governance-risk-compliance-grc**

www.hcltech.com

BI-112257745735-EN00GL