asureti

Asureti Compliance Brief: Third Party Risk Management

Third Party Risk: In Brief

> *Have we identified our third parties?*
>
> *What data are we sharing?*
>
> *What do we need to do?*

Whether it is referred to as third-party risk, vendor management, supply chain management, or something else, organizations must recognize the **risks of operating as an extended enterprise.** Today's interconnected business models enable companies to leverage partnerships to manage costs and increase competitive advantage.

The risks this sharing process poses to those assets include security protections and associated breach risk, availability standards and associated operational risk, ownership rights and associated strategic risk, and other key risk points across financial, operational, reputational, and legal areas.

Considering these risks and evolving business operations — alongside an increasingly complex regulatory landscape — **third-party governance and oversight models are a must-have for organizations.**

What do we need to do?

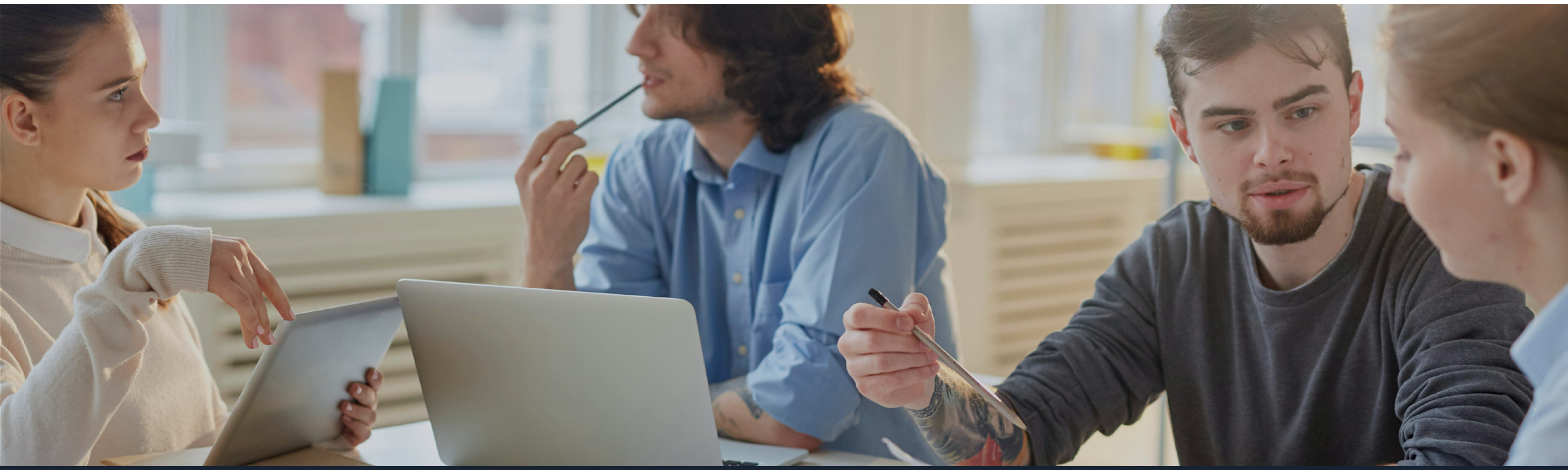
Leverage a risk-based action plan to assess data sharing, services provided, and monitoring structures to determine necessary steps for appropriate risk management.

Common review elements may include:

- **Information Security:** Technical configurations, security architecture, access management, monitoring, and incident response.
- **Physical Security:** Facility access, security monitoring, and document control measures.
- **Policies & Programs:** Program and governance models, policies and standards, and reporting structures.
- **Human Resources:** Background checks/verifications and associate training programs.
- **Availability:** System maintenance and monitoring process, support and operational oversight, system change processes.
- **Business Continuity:** Disaster recovery and business resumption plans.

The following structured activities will aid in determining required actions:

- **Establish Governance / Program Structure**
- **Establish Operational Vendor Partner Life Cycle Management**
- **Assess Data Protection Risk Management**
- **Leverage Technology Integrations**



Asureti's Third Party Risk Management **Framework**

GOVERNANCE / PROGRAM STRUCTURE

A governance and program standard, incorporating policy, classification structures, and ongoing monitoring functions, will establish the baseline and **framework that integrates functions across the organization to support management of external partners.** Key to appropriate governance is identification of third parties utilized by the organization. A risk rating or classification structure will then include assessment of data being shared, nature of the vendor's operations, potential customer impact, regulatory considerations, and level of dependency on the vendor for ongoing operations (e.g., system availability or other operational requirements).

OPERATIONAL VENDOR PARTNER LIFE CYCLE MANAGEMENT

A full vendor management program includes the **entire life-cycle process for managing vendor relationships** — from planning and selection to ongoing monitoring. This includes assigning responsibility for relationship management, contract management processes, and service level monitoring.

DATA PROTECTION RISK MANAGEMENT

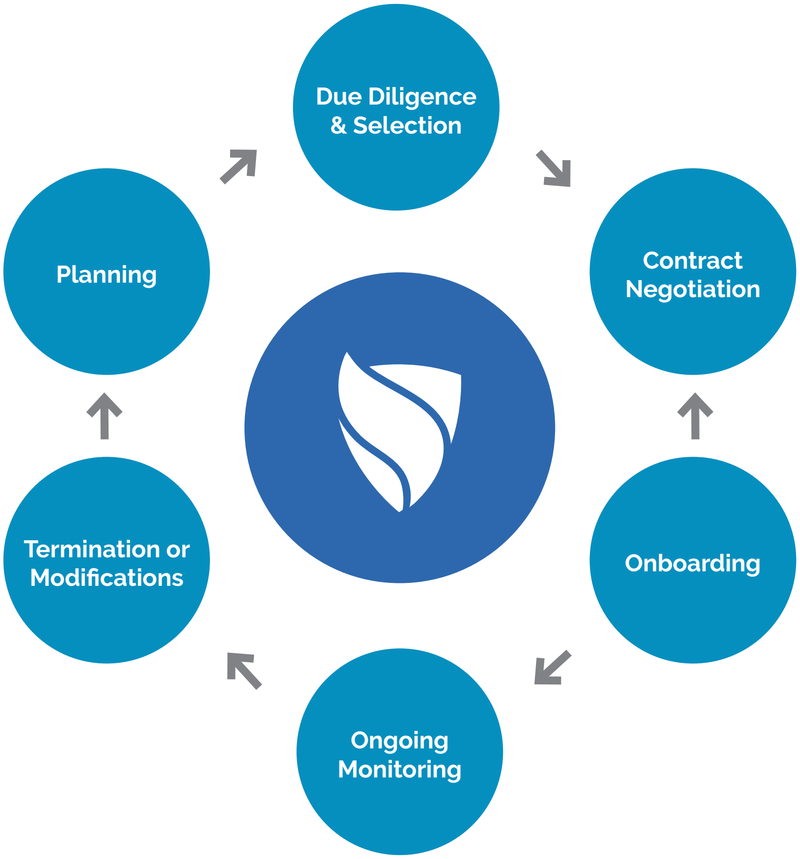
Specific activities for monitoring and validation of vendor data protection practices must be **aligned with organizational requirements;** however, certain focus areas are appropriate for most companies. Key requirements may apply for specific data types or industries; the Health Insurance Portability and Accountability Act and General Data Protection Regulation are key examples of regulations including specific requirements in regard to third parties.

TECHNOLOGY INTEGRATIONS

This component includes implementing and operating key systems to **enhance effectiveness, efficiencies, and communication** within the Vendor Management Framework. Leveraging appropriate tools can provide for streamlined processes and reporting of third-party risk.

Third Party Management **Lifecycle**

Accountability | Oversight | Monitoring | Risk Management



1. Planning

The standard process to obtain strategic requirements for a new (current) third party relationship.

2. Due Diligence & Selection

Procurement, the relationship manager and business / functional areas conduct risk based due diligence on applicable potential third parties before selecting and entering into contracts or relationships.

3. Contract Negotiation

The established processes to ensure that new contracts capture the risks appropriately, appropriate reviews and approvals are completed, and periodic assessments of current contracts are completed against company standards.

4. Onboarding

Once contracted, Procurement notifies AP to setup the vendor. Additional due diligence by Audit, Security, or Compliance functions may be conducted to confirm processes, controls, and servicing are effective prior to implementation of the service.

5. Ongoing Monitoring

The relationship manager and Procurement will implement processes to ensure oversight activities are in place based on key risk factors for each vendor. Security and Compliance teams will ensure appropriate data protection monitoring.

6. Termination or Modifications

Vendor relationships may be modified or ended when required due to a variety of reasons. Business / functional areas must have appropriate plans in place to transition activity if needed based on the products and/or services being provided.

Core Functional Considerations

- ✓ Shared risk management platform to manage, track, and report on information related to the company's vendors
- ✓ Identify high risk vendors through risk rating, tiering, and classification structure
- ✓ Establish company-standard assessment processes and contents
- ✓ Automate vendor assessments (questionnaires, follow-ups, and findings management)
- ✓ Business Management ownership and transparency for vendor information
- ✓ Link to controls, findings, and risks – integrated information and reporting