PURPOSE

To achieve operational and strategic goals, CVS Health relies on Third Parties for a variety of purposes. While utilizing these Third Parties brings multiple benefits to CVS Health, the engagement of these Third Parties can also present risk exposing CVS Health to regulatory actions, financial penalties or loss, reputational harm, market share decline, regulatory and legal action, or other negative impacts. As such, all CVS Health employees and CVS Health’s Agents that engage Third Parties are responsible for ensuring that all Third Party interactions and activities are conducted in a sound manner and in compliance with applicable laws, regulations, and CVS Health standards.

The purpose of this Policy is to define CVS Health’s guiding principles with respect to Enterprise Third Party Risk Management (“ETPRM”) to effectively manage the risk presented by any Third Party providing services to CVS Health.

**SCOPE**

This document establishes policies and procedures for all CVS Health Business Units to follow in engaging Third Parties. It also provides the foundation and principles for Business Units to develop corresponding procedures commensurate with their strategies and business activities.

As a good business practice, and consistent with past practices, CVS Health has established a program to review and assess Third Parties who provide or intend to provide non-resale services or goods to CVS Health.

The ETPRM program facilitates comprehensive review and assessment across applicable CVS Health risk domains for Third Parties and provides a centralized repository for documenting In Scope Third Party attributes and security controls. Assessment of Third Parties is conducted through the coordinated efforts of Procurement, Third Party Risk Governance, Legal and other relevant departments, depending on the level of potential risk presented by the engagement with the In Scope Third Party.

1. **In Scope Third Party Types**

For the purposes of this Policy document, “Third Party” is defined as: a) individuals and/or entities with whom CVS Health engages and/or transacts with for products, materials, technologies, goods, or services, across both indirect and direct channels; b) individuals and/or entities that sell, re-sell, and/or distribute CVS Health products; c) entities that CVS Health shares, processes, transmits, stores, or has access to proprietary, confidential or sensitive member data for research purpose and/or d) Third Parties who CVS Health has fully outsourced to an activity that is critical to its ongoing operations.

1. **In Scope Third Party Risk Domains**

To properly assess and manage risks presented by the use of Third Parties, CVS Health has identified key risk focused areas, used to identify, assess, and validate controls in accordance with each area’s standards. These are referred to as Risk Domains:

The following Third Party Risk Domains are in scope for this Policy:

· Business Resiliency Risk

· Contract Risk

· Data Privacy Risk

· Data Protection and Physical Security Risk

· Regulatory and Compliance Risk

**POLICY**

1. **Business Relationship Owner**

Business relationship owners who engage, interact with, or utilize Third Parties (“Business Relationship Owners”) are responsible for ensuring that Third Parties are assessed by ETPRM. This Policy applies to all current and potential Business Relationship Owners involved in any or all the Third Party Engagement Lifecycle activities such as, planning, due diligence, contracting, continuous monitoring, and/or renewal or termination of Third Party Engagements. The Primary factor for determining who has accountability of a Third Party Relationship is risk. The risk is carried by the Business Relationship Owner that has made the determination to outsource an activity or leverage a particular Third Party to provide a product or service.

Business Relationship Owners adherence to this Policy, as well as exercising good judgment and sound decision making, will support better overall management of the risks presented by Third Party Engagements.

Business Relationship Managers are the individuals who are the primary CVS Health contacts for specific Third Party Engagements and are ultimately responsible for managing risk associated with their Third Party Engagements. Business Relationship Managers are also responsible for understanding the contractual obligations of both CVS Health and the Third Party and ensuring that they are met. Business units are responsible for enabling the Business Relationship Managers to be compliant with the following responsibilities and any other obligations set forth in this Policy.

**Key Responsibilities**

1. Own the risk of the relevant Third Party Engagement (also responsible to identify a transition plan if a change in circumstance (e.g., role change) requires a change in risk ownership).
2. Identify and properly assist in remediation efforts of risks identified and presented to CVS Health by Third Party Engagements.
3. Submit accurate and complete information about Third Parties in accordance with ETPRM program requirements.
4. Respond to all ETPRM documentation requests in an accurate, complete, and timely manner.
5. Ensure that the Inherent Risks associated with the reliance on Third Party storing, processing, and transmitting of CVS Confidential or Restricted Information are identified, documented, and mitigated to an acceptable Residual Risk level prior to commencement of an engagement or execution of a contract.
6. Work with ETPRM, applicable Risk Domain SMEs, and the Third Party to remediate and close all contingencies and risk findings resulting from Due Diligence conducted on the Third Party Engagement to ensure the Third Party adheres to controls and at an acceptable Residual Risk level prior to commencement of an Engagement.
7. Proactively monitor the Third Party Engagement to identify risk and manage all identified risk throughout the Third Party Engagement Lifecycle.
8. Participate in the assessment or re-assessment of the Third Party Engagement to the extent required by ETPRM.
9. Promptly report to ETPRM any material changes to the Third Party attributes, Engagement, Risk, or level of access to Confidential or Restricted Information.
10. Conduct termination activities/tasks as required and in accordance with ETPRM guidance, to ensure shared data is properly destroyed or returned to CVS Health.
11. **Third Party Engagement Lifecycle**

To enable a cohesive approach and appropriate oversight throughout the entirety of a Third Party Engagement, Business Relationship Owners must follow the Enterprise Third Party Risk Management Lifecycle when engaging Third Parties.

1. **Initial Intake and Pre-Engagement**

At the Initial Intake & Pre-Engagement stages, Business Relationship Owners are required to identify the Inherent Risk, perform further due diligence to better understand and manage the potential risk posed by the Third Party Engagement. The Business Relationship Owners are required to conduct planning activities commensurate with the level of risk and complexity of the Third Party relationship, assessing the volume of activity, potential for subcontractors, technology needed, and use of potential offshore support. Required activities must be documented and completion of the Inherent Risk Assessment prior to contract signing.

1. **Contracting and Onboarding**

At the Contracting and Onboarding stage, Business Relationship Owners are required to follow the approved contracting process for each respective Third Party. This includes, but is not limited to, engaging Procurement and the applicable risk SMEs (e.g., Privacy, Security, Compliance, Legal) to support and/or drive Contract drafting and leveraging only approved contract templates. Contract clauses/provisions must be properly documented and in alignment with Third Party Risk Management activities (i.e., completion of required assessments/right to audit, SLAs, Business continuity plans, etc.).

1. **Management and Monitoring**

At the Management and Monitoring stage, Business Relationship Owners are required to understand and comply with their ongoing risk management and monitoring responsibilities for their Third Party Engagements, including proactive identification and mitigation of risk.

**d. Issue Management**

Through ongoing monitoring activities required to be perform by the Business Relationship Owner (Security Assessments, Third Party Review, etc.) risks identified and associated with the Third Party service, must be properly documented in Archer. The Business Relationship Owner must work with the Third Party to establish action plans and target dates to remediate risks identified. Risks that cannot be remediated and the Business Relationship Owner deems acceptable, should be escalated, and properly reviewed by the Risk Domain Review Group (“RDRG”).

1. **Renewal or Termination**

At the Termination or Renewal stage, Business Relationship Owners are required to understand and comply with their responsibilities in relation to the Renewal and/or Termination of Third Party Engagements (e.g., risk re-assessment of the Third Party prior to renewal of the contract, completion of required termination checklists if a contract will not be renewed). Business Relationship Owners should develop termination and exit plans to ensure the business can exit and/or transition activities to another Third Party or have the capability to bring services in-house.

In addition, Business Relationship Owners should ensure that all CVS Health data and property are returned and/or destroyed in accordance with applicable data retention requirements. If a third party is unable to return data, they should provide an attestation in writing that the data has been removed from all systems and all physical records have been properly destroyed.

1. **Training and Awareness**

Training is an essential part of the Enterprise Third Party Risk Management program and was developed to provide guidance on properly managing Third Party Relationships in accordance with established guidelines, to Business Relationship Owners. Training is available through the Training -Leaning Hub and will be administer to appropriate CVS Health personnel. Business areas and Risk domains should establish additional training as needed

1. **Consequences of Non-Compliance**

Failure to comply with CVS Health Policies and Procedures is a violation of the CVS Health Code of Conduct. Any CVS Health Business Relationship Owner who violates this Policy will be subject to sanctions, up to and including termination of their employment, in accordance with the CVS Health Code of Conduct.

Any CVS Health Colleague who is aware of any violation or potential violation of this Policy shall promptly report any concerns to the CVS Health Legal Department.

**PROCEDURE**

Each Business Relationship Owner is required to engage the ETPRM process at least \_\_ days prior to project start to allow sufficient time for review and assessment to take place. No work by a Third Party shall commence and no contract shall be executed until prior to the completion of the appropriate procedures as stated in this Policy.

1. **Process Flow Overview**

The following Process Flow Overview Description walks through each step of the ETPRM Third Party Engagement Assessment Management Process:

* 1. **Third Party Engagement Intake**

A new Third Party Engagement will be entered in the Archer ETPRM module in one of two ways:

(1) An SAP Ariba Contract Workspace is created for a new Third Party Engagement and includes a Privacy/Security Risk value of “Risk Review Required”, automatically initiate the Third Party Engagement in the Archer ETPRM module; OR,

(2) Direct Third Party Engagements outside the scope of the Non-Merchandise Purchases Policy and not entered into SAP Ariba may be manually entered into Archer by the Business Relationship Owner.

* 1. **Inherent Risk Assessment Completion**

The Business Relationship Owner will automatically be assigned and notified through Archer to the complete an Inherent Risk Assessment when the Third Party Engagement information has been entered. The Business Relationship Owner or a delegate will complete the Inherent Risk Assessment questions, detailing various specifics about the Third Party and the Engagement.

Risk scoring logic has been applied to Inherent Risk Assessment responses to identify known risks related to each Risk Domain, which compose an overall Inherent Risk Score. The Risk Scores will help drive the Inherent Risk Assessment disposition of Third Party Engagements but are not dispositive.

* 1. **Due Diligence Assessment**

Risk Domains will ask questions of the Third Party and require certain evidentiary documentation of controls. The depth of this scrutiny will depend on the nature of the Third Party and the relevant Engagement.

* 1. **Risk Domain Review Group**

The Risk Domain Review Group (“RDRG”) is composed of stakeholders from relevant CVS Health departments that serve as Subject Matter Experts on a given Risk Domain.

Each Risk Domain Owner is tasked with ensuring issues and risks are properly identified and corrected as part of the ETPRM process. Risk Domain Owners are responsible for the inclusion and upkeep of Inherent Risk Assessment questions, Due Diligence questions, and assistance with the development of remediation and/or corrective action plans.

RDRG review Third Party Engagements as well as the Findings & Corrective Action Plans when Business Relationship Owners would like to proceed with a Third-Party Engagement that would otherwise be “Denied” due to not meeting specific control requirements or an acceptable Residual Risk level.

* 1. **Re-Assessment**

All Third Party Engagements that go under initial assessment are subject to re-assessment on a periodic basis dependent on their risk level.

Third Party Engagement Re-Assessments will be kicked off through the Archer ETPRM module approximately 45 days prior to the commencement of a re-assessment (if found to be required).

All Third Party Engagements that come up for re-assessment will trigger a notification to the Business Relationship Owner on record to attest to the previous Inherent Risk Assessment or complete a new one if the Third Party Engagement has changed.

If the Third Party Engagement is no longer active, the Business Relationship Owner will be asked to enter a new contract date in the Archer ETPRM Module.

**Other Applicable Third Party Risk Policies:**

[Information Governance Policy](https://policy.corp.cvscaremark.com/pnp/faces/DocRenderer?documentId=DOC-063180) (DOC-063180)

[Information Security Policy (CIST-0004)](https://policy.corp.cvscaremark.com/pnp/faces/DocRenderer?documentId=CIST-0004)

[Third Party Risk Governance Policy CIST-066129](https://policy.corp.cvscaremark.com/pnp/faces/DocRenderer?documentId=CIST-066129)

Data Classification Standard (RMGT-046805)

For full details on when a Contract is required when engaging third parties, please refer to the CVS Health Contracts Policy (CPUR-0002)

[Non-Merchandise Purchases Policy](https://policy.corp.cvscaremark.com/pnp/faces/DocRenderer?documentId=CPRO-0005) (CPRO-0005)

[Merchandising – Category Management: Setting Up and Maintaining a Supplier](https://policy.corp.cvscaremark.com/pnp/faces/DocRenderer?documentId=DOC-052074) (DOC-052074)

[Enterprise Response and Resiliency (ERR) – Third Party Business Resiliency](https://policy.corp.cvscaremark.com/pnp/faces/DocRenderer?documentId=DOC-049250)

**DEFINITIONS**

**Agent:** An individual or organization authorized to engage Third Parties on CVS Health’s behalf.

**Archer:** The automated Enterprise application utilized by ETPRM as system of record for Third Party risk management and submission and processing of inherent risk assessments, risk scoring, final determinations, and issues management.

**ARIBA:** The automated cloud platform system utilized by Enterprise Procurement for submission and processing of contract requests, agreements, purchase requisitions, purchase orders, and invoices.

**Business Relationship Owner:** The individual who is the primary CVS Health contact for an Engagement with a Third Party; Any CVS Health employee and/or Agent (where permitted) that engages Third Parties, and as such will be involved in any or all the Third Party Engagement Lifecycle activities such as, planning, due diligence and selection, contracting, contract management, ongoing monitoring, and/or renewal/termination of Third Party Engagements.

**Confidential Information**: Refers to information that CVS Health must maintain the confidentiality and ensure its security, including Personally Identifiable Information (PII), which incorporates Protected Health Information (PHI), Cardholder Data (CHD), or Employee Employment Data, and Proprietary Information, which incorporates Financial Records, Intellectual Property, and Protected Business Data. This means such information requires Enhanced Safeguarding. Under Enhanced Safeguarding, dissemination of Confidential Information is highly limited to those workforce members and third parties with a clearly defined need to know. A need to know is a demonstrable, compelling, and authorized business need for accessing and using such information.

**Contract:** A Contract as used in this policy shall include, but not be limited to, Purchase Agreement, Service Agreement, Master Agreement, Professional Service Agreement,

Statements of Work, Hosting Agreement, License Agreement, Subscription Agreement, Consulting Agreement, Software Agreement, Business Associate Agreement, and Mutual Non-Disclosure Agreement, Software as a Solution Agreement.

**Contract Risk:** Risk exposure arising due to the Third Party being unable or unwilling to accommodate or comply with contract clauses / terms & conditions that enable CVS Health’s oversight, and transparency into, the Third Party's performance, risk, and compliance capabilities.

**CVS Health:** CVS Health Corporation and each of its subsidiaries and affiliates.

**Data Privacy Risk:** Risk exposure arising to due to a Third Party’s access, usage, and/or possession of Confidential and/or Restricted information.

**ETPRM Program Team:** Enterprise group primarily responsible for the ongoing development and facilitation of CVS Health’s ETPRM Program.

**Inherent Risk:** an assessed level of raw or untreated [risk](https://en.wikipedia.org/wiki/Risk); that is, the natural level of risk inherent in a process or activity without doing anything to reduce the likelihood or mitigate the severity of a mishap, or the amount of risk before the application of the risk reduction effects of controls.

**Regulatory & Compliance Risk:** Risk exposure arising due to non-compliance with regulatory requirements associated with the products / services provided by a Third Party and / or the CVS Health products / services the Third Party is supporting, resulting in possible regulatory actions, financial penalties, or loss of stakeholder confidence.

**Residual Risk**: the amount of [risk](https://en.wikipedia.org/wiki/Risk) or [danger](https://en.wikipedia.org/wiki/Risk) associated with an action or event remaining after natural or [inherent risks](https://en.wikipedia.org/wiki/Inherent_risk) have been reduced by risk controls.

**Restricted Information**: Information or data where legal, regulatory, or contractual relations mandates the highest level of security protection. CVS Health is required to protect data that is regulated by but not limited to HIPAA, HITECH, PCI DSS.

**Risk Domain:** Key risks identified by CVS Health that are presented by Third Party Engagements

**Risk Domain Owner:** The enterprise owner of a respective risk domain and relevant frameworks.

**Security Risk:** Risk exposure arising due to Third Party’s access of CVS Health’s data, network, and/or physical space to provide products / services.

**Third Party:** a) individuals and/or entities with whom CVS Health engages and/or transacts with for products, materials, technologies, goods, or services, across both indirect and direct channels; b) individuals and/or entities that sell, re-sell, and/or distribute CVS Health products; and c) entities that CVS Health shares member data with for research purposes. Healthcare providers and payers who are subject to the [Health Insurance Portability and Accountability Act](https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996)(HIPAA), and interact with CVS for Treatment, Payment and Healthcare Operations are not In Scope Third Parties.

**Third Party Engagement**: A single service provided to, or individual contract with an CVS Health business unit.

**Third Party Engagement Lifecycle:** The end-to-end view of engagement activities from Initial Intake to Termination or Renewal.

**REVIEW AND REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Revision No.** | **Reason for Change** | **Sections Affected** |
|  | 1.00 | New Document | N/A |