This is a document for VendorWatch stakeholders that explains the purpose, scope, mission, and approach of the accompanying vendor assessment report.

Purpose

Classify the vendor based on:

- Likelihood of the vendor providing inadequate service levels.
- Likelihood of the vendor compromising the organization's data
- Impact of the vendor not meeting the organization's requirements.
- The criticality of the vendor's services or products to the organization.

Identify missing or inadequate security controls to maintain agreed-upon service levels and protect the confidentiality of the organization's data.

Collect and archive important vendor information:

- General information about the vendor
- The services or products the vendor provides
- Vendor contacts
- Contracts and agreements
- Evidence of implemented security controls

Measure and communicate the vendor risk to the organization.

Scope

There are multiple areas where vendor deficiencies threaten service levels and privacy. VendorWatch evaluates the following areas.

- Policies and processes
- Regulatory compliance
- Security and privacy controls
- Business continuity and recovery plans
- Breach disclosure
- Service level agreements
- Financial stability
- Vendor location

Mission

The third-party risk assessment tool VendorWatch identifies vendor security gaps. The application evaluates the vendor's controls, policies, and processes that could impact business delivery, reputation, and competitiveness.

Using defined benchmarks, this assessment is part of an ongoing process to gauge the vendor's current state. VendorWatch manages progress monitoring to ensure the vendor adheres to requirements. This risk management process aims to reduce the probability of loss or significant reduction of the availability of critical services or products. Another goal is to reduce unauthorized personal data or trade secret disclosure. VendorWatch assists in meeting those goals.

The evidence-based information and analysis VendorWatch provides allows stakeholders to make informed decisions regarding vendor options.

Approach

VendorWatch manages the evaluation, the roadmap to improvement, and sustained adherence to standards. The approach is based on the ISO 31000 risk management process consisting of six cyclical phases.

Phase 1 – Establish Context: The organization identifies a vendor that requires assessment. Vendor contacts knowledgeable of the vendor's existing security controls, policies, and processes provide information and evidence.

Phase 2 – Risk Identification: VendorWatch distributes checklist surveys to the vendor contacts to identify if all the vendor's required controls are in place. These vendor contacts answer the survey questions. The contacts also provide additional commentary, documentation, and visual evidence. Visuals include photographs, screenshots, diagrams, or charts.

Phase 3 – Analysis: VendorWatch processes the completed survey data for analysis. Survey question weighting measures the impact of responses deemed non-compliant with security requirements.

Phase 4 – Evaluation: VendorWatch identifies security and compliance gaps based on the survey results. VendorWatch computes a Vendor Risk Score based on the vendor's:

- Criticality to the organization's business functions.
- Potential consequence services or products being unavailable.
- Likelihood of threat actors targeting the vendor.
- General reliability the vendor has historically provided.
- Vulnerability due to not meeting security standards.

The organization can compare the Risk Score against a predetermined risk tolerance level to determine what remedial action the vendor should take to do business with the organization. The organization can also compare the Risk Score with competing vendors to rank them based on risk.

Phase 5 – Treatment: The organization prescribes remedial recommendations for the vendor and develops an action plan managed through VendorWatch.

Phase 6 – Monitor: The organization conducts periodic reassessments to monitor the continued adherence to standards and the maintenance of compliance.