**ADM 417**

**APPENDIX D – NEW PRODUCT EVALUATION FORM**

|  |  |
| --- | --- |
| **Procedure** | **Notes** |
| **General Information** |
| Summary of product or service |  |
| Proposed vendor(s) |  |
| Review date |  |
| Individual(s) performing the review |  |
| Date review documentation and contract presented to Management |  |
| Date regulator notification provided (for financial institutions)  |  |
| Date of relevant policy updates  | *<Consider risk assessments, IS Program, IT Policy, Incident Response, Business Continuity and Disaster Recovery, etc.>* |
| **Relationship to Strategic Plan** |
| *
 |
| **Benefits** |
| *
 |
| **System/Data Hosting**  |
| *
 |
| **Costs** |
| *
 |
| **Potential Compliance, Privacy and/or Legal Issues** |
| *
 |
| **Target Implementation Timeframe** |
| *
 |

**NEW VENDOR EVALUATION FORM**

**Vendor Evaluation**

The following list contains many items that may be re viewed and analyzed as part of due diligence procedures.

|  |  |  |
| --- | --- | --- |
| **Completed** | **Item Reviewed** | **Responses and Notes** |
|  | Audited financial statements, annual reports, SEC filings, and other available financial indicators |  |
|  | Experience and ability to implement and monitor the proposed activity |  |
|  | Experience and ability in implementing and monitoring the proposed activity |  |
|  | Business reputation, status in the industry, and sustainability  |  |
|  | Qualifications, training, and experience of the company’s principals and staff |  |
|  | Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies |  |
|  | Existence of significant complaints, litigation, or regulatory actions against the company |  |
|  | Ability to perform the proposed functions using current systems or the need to make additional investments |  |
|  | Use of other parties or subcontractors  |  |
|  | Scope of internal controls, information security (systems and data security), privacy protections, and audit coverage (vulnerability testing) |  |
|  | Business resumption strategy and contingency plans (to include pandemic planning and relevant threats such as DDoS) |  |
|  | Adequacy of data security policies (to include location, encryption, segregation, end-user logical access controls, and recovery information)  |  |
|  | Knowledge of relevant consumer protection regulations and civil rights laws  |  |
|  | Adequacy of management of information systems |  |
|  | Insurance coverage (focus on cybersecurity preparedness)  |   |
|  | Eligibility to perform as a service provider given the existence of any outstanding enforcement actions against the third party and the requirements of Section 19 of the FDI Act that may apply to Organization-affiliated parties |  |
|  | Record retention and maintenance practices  |  |
|  | Identification of potential conflicts of interest |  |
|  | Impact of proposed contracts on the third party’s operations and financial condition |  |