

Bank Secrecy Act (BSA) / Anti-Money Laundering (AML) Risk Assessment

**APPROVED BY**

Acme, LLC dba Initech Vending BSA Officer

Acme, LLC dba Initech Vending Board of Directors

**TABLE OF CONTENTS**

OVERVIEW 3

Introduction 3

Initech Profile 3

Methodology 4

Inherent Risk 5

*Customers and Entities* 5

*Products/Services* 5

*Geographic Locations* 6

Inherent Risk Ratings 6

Mitigating Controls 6

Residual Risk 8

Results 8

ANALYSIS AND RESULTS BY RISK CATEGORY 9

Customers and Entities 9

Inherent Risk 9

*Customer Base - Foreign* 9

*Customer Base - Domestic* 10

*Customer Types* 10

*Change in Customer Base* 11

Mitigating Controls 11

Residual Risk 12

Products/Services 12

Inherent Risk 12

*DASH Kiosks, DASH In – Cash Out* 13

*DASH Kiosks, Cash In – DASH Out* 13

*Anticipated Transactional Activity* 13

Mitigating Controls 14

Residual Risk 14

Geographic Locations 15

Inherent Risk 15

Mitigating Controls 16

Residual Risk 17

TRENDING AND DIRECTION OF RISK 17

RECOMMENDATIONS 17

Customers and Entities 17

Products/Services 18

Geographic Locations 18

SENIOR MANAGER APPROVAL 18

# **OVERVIEW**

## **Introduction**

Pursuant to the United States (U.S.) legal and regulatory requirements, including the Bank Secrecy Act (BSA) as amended by the USA PATRIOT Act, regular anti-money laundering (AML) risk assessments are vital components of an effective BSA/AML program. Well-developed risk assessments will serve to facilitate an overall understanding of the risk profile of Acme, LLC dba Initech Vending (“Initech”) as it relates to money laundering and terrorist financing activities; assist Initech in the application of appropriate risk management policies, procedures, and other internal controls; and drive any necessary BSA/AML program enhancements.

The purpose of this Risk Assessment is to inform the Board of Directors[[1]](#footnote-1) (“Board”) of the risk profile of Initech. By examining the composition of Initech’s customer base, geographic footprint, and products and services offered, this Risk Assessment will assist the Board in understanding where risks related to BSA/AML compliance lie. This assessment includes: (a) an evaluation of the adequacy and appropriateness of the policies and controls established by Initech in order to comply with the Bank Secrecy Act and mitigate the associated risk; (b) identification of any significant gaps or weaknesses; and (c) recommendations for improvements that will serve to strengthen Initech ’s overall BSA/AML Program.

### **Initech Profile**

Initech is a registered money services business (MSB) that operates two automated DASH kiosks (“kiosks”). As of November 1, 2016, Initech reported a net worth of approximately $30,000, the majority of which consists of hardware and revolving liquidity in DASH currency sufficient to service the kiosks.

Initech is headquartered in Boulder, Colorado. Initech’s company operations are domestic in nature; no foreign operations, products, or services (i.e. transactions) are offered.

Initech operates two kiosks, one unidirectional or “one-way” kiosk, and one bidirectional or “two-way” kiosk. The unidirectional kiosk exchanges user U.S. Dollar-denominated cash (or ‘fiat money’) for DASH-denominated cryptocurrency. The bidirectional kiosk exchanges both user U.S. Dollar-denominated cash for DASH-denominated cryptocurrency, and user DASH-denominated cryptocurrency for U.S. Dollar-denominated cash.

The kiosks occupy dedicated space within third-party establishments. Initech operates and is solely responsible for the servicing of the kiosks.

Initech has a written BSA/AML Program that has been approved by the Board. The BSA/AML Program establishes the framework and expectations for Initech’s BSA/AML compliance and serves to minimize the risk of money laundering and terrorist financing by establishing:

* Governance, roles, and responsibilities
* Designation of an individual responsible for BSA Compliance
* A system of internal controls
* An ongoing employee training program
* Independent testing

The Board approves Initech’s BSA/AML Program on an annual basis.

Initech’s written BSA/AML Program describes how Initech achieves the requirements set forth within the Board-approved BSA/AML Policy. The BSA/AML Program is risk-based and commensurate with Initech’s BSA/AML risk profile. It highlights the day-to-day processes that Initech follows in an effort to minimize the risk of money laundering and terrorist financing. The Board approves Initech’s BSA/AML Program on an annual basis or when significant changes have been made to the Program.

Initech’s BSA/AML Program outlines the requirements and expectations surrounding independent testing. Independent testing will be completed every twelve (12) months by qualified persons and, at a minimum, shall include:

* An evaluation of the overall adequacy and effectiveness of the BSA/AML Program, including policies, procedures, and processes.
* A review of Initech’s Risk Assessment for reasonableness given Initech’s risk profile (customers and entities, products and services, and geographic locations).
* Appropriate risk-based transaction testing to verify Initech’s adherence to recordkeeping and reporting requirements (e.g., SARs and CTRs).
* An evaluation of management’s efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable.
* A review of staff training for adequacy, accuracy, and completeness.
* A review of the effectiveness of suspicious activity monitoring (manual, automated, or a combination).
* An assessment of the overall process for identifying and reporting suspicious activity.

Auditors document the audit scope, procedures performed, testing completed, and findings of the review. All audit documentation and work papers are available for examiner review. Any violations, policy or procedure exceptions, or other deficiencies noted during the audit are included in an audit report and reported to the Board in a timely manner. The Board and the audit staff track audit deficiencies and document corrective actions.

It is the responsibility of the BSA Officer to make sure any identified deficiencies are documented, tracked, and corrected. The BSA Officer will determine if any action plan, corrective actions, or both are appropriate and acceptable.

### **Methodology**

For the 2016 BSA Risk Assessment, Initech utilized a methodology that consisted of both qualitative and quantitative analysis and is comprised of a combination of a rating and points system. Individual risk factors or controls are given initial ratings that are then assigned corresponding point values. These point values are then averaged to determine overall category ratings and ultimately the overall company-wide rating. Risk factors, controls, or both may be weighted as appropriate. The methodology outlines specific inherent risk and mitigating control categories to be evaluated and ultimately provides for the determination of Initech’s overall residual AML risk. Each of these components is explained in greater detail below.

### Inherent Risk

The inherent risk is the level of risk present, absent any mitigating controls. Regulatory guidance, Initech’s business strategy, operating model, and volumetric considerations were all factored in determining the level of inherent risk present within each risk category. The Federal Financial Institutions Examination Council (FFIEC) Manual sites specific risk categories to consider when assessing Initech’s risk. These risk categories, which were evaluated as part of this year’s assessment, are as follows:

* Customers and Entities
* Products/Services
* Geographic Locations

### *Customers and Entities*

This category is intended to illustrate the composition of Initech’s customer base in order to determine the level of inherent risk posed by Initech’s customers. The following individual risk factors are included in this category:

* Customer Base Geography/Foreign Locations - This factor is used to identify the number of customers and entities residing or operating in foreign locations. Regulatory guidance suggests customers and entities residing or operating in foreign locations, especially those in higher risk jurisdictions, may pose a higher risk of money laundering or terrorist financing.
* Customer Base Geography/Domestic Locations - This factor is used to identify the number of customers and entities residing or operating in high risk domestic locations. Regulatory guidance suggests customers residing in high risk domestic locations may pose a higher risk of money laundering or terrorist financing. High risk domestic locations include those designated as High Intensity Financial Crime Areas (HIFCAs) and High Intensity Drug Trafficking Areas (HIDTAs).
* Customer Type - This factor is used to identify customer types that may pose a higher AML risk such as Politically Exposed Persons (PEPs), Money Services Businesses (MSBs), and non-profit organizations or charities, for example. Regulatory guidance suggests certain customer types, including, but not limited to those mentioned previously, may pose a higher risk of money laundering or terrorist financing.
* Customer Base Changes - This factor is used to identify potential or anticipated changes in Initech ’s customer base (e.g. geographic location of customers, customer types, etc.) that may result in a change in the level of money laundering or terrorist financing risk present.

### *Products/Services*

This category is intended to identify the products and services offered by Initech and determine the level of inherent risk associated with each. Regulatory guidance suggests certain products and services may pose a higher risk of money laundering or terrorist financing depending on their specific nature. Those that allow for the rapid movement of funds, transactions involving foreign locations, or user anonymity are considered to be of heightened risk.

### *Geographic Locations*

This category is intended to identify the geographic locations in which Initech operates and determine the level of inherent risk associated with those locations. This includes both where Initech has physical operating centers, as well as where transactions occur. Individual risk factors included in this category are:

* Foreign Operating Locations - This factor is used to identify any foreign locations, especially high risk jurisdictions, in which Initech maintains an operating center.
* Domestic Operating Locations - This factor is used to identify any high risk domestic locations (HIFCAs and HIDTAs) in which Initech maintains an operating center.
* Foreign Transaction Locations - This factor is used to identify any foreign locations, especially high risk jurisdictions, in which transactions occur.
* Domestic Transaction Locations - This factor is used to identify any high risk domestic locations (HIFCAs and HIDTAs) in which transactions occur.

### Inherent Risk Ratings

The level of inherent risk present for each applicable risk factor was determined as described above and assigned a rating of Low, Medium, or High based on the definition provided in the table below.

|  |  |
| --- | --- |
| **Risk Rating** | **Definition** |
| Low | Risk is “Low” when a customer, service, or geography contains minimal inherent risks irrespective of any consideration for internal controls intended to mitigate relevant regulatory, financial, or reputation risks. |
| Medium | Risk is “Medium” when a customer, service, or geography contains some inherent risks before the threat of financial loss, regulatory exposure, or damage to the reputation of the organization is mitigated. |
| High | Risk is “High” when a customer, service, or geography contains significant inherent risks before considering mitigating controls. The threat of financial loss, regulatory exposure, or damage to reputation of the organization is significant. |
| N/A | The risk factor is not applicable to Initech. |

The assessed rating for the individual risk factors within a risk category were assigned corresponding point values of 1=Low, 2=Medium, and 3=High and averaged to determine the inherent risk rating for the risk category as a whole. The inherent risk ratings for each risk category were subsequently averaged to determine Initech’s overall inherent risk rating.

### Mitigating Controls

Mitigating controls are risk management activities, factors, and/or considerations that serve to mitigate or reduce the level of inherent risk present. There were six general categories of mitigating controls assessed, as applicable, for each relevant risk factor or risk category. The categories of mitigating controls are as follows:

* Governance and Oversight - This category refers to the reporting structure, oversight, and management of Initech’s overall program.
* Policies and Procedures - This category refers to the appropriateness and applicability of Initech’s written BSA Program, policies, and corresponding procedures.
* Surveillance and Reporting - This category refers to the appropriateness and applicability of Initech ’s monitoring processes used to detect suspicious activity that may indicate money laundering or terrorist financing activities. This category also refers to processes in place to ensure adherence to reporting requirements related to suspicious activity and CTR reportable events.
* Training - This category refers to one of the four pillars of an effective AML Compliance Program and is intended to assess the appropriateness and adequacy of Initech’s AML training program. AML training should be designed to improve the knowledge, performance, and skills of Initech’s employees. A comprehensive training program helps prepare employees to detect and report customers who may be using products and services to engage in unlawful activity.
* Testing and Monitoring - This category refers to testing and monitoring activities in place designed to ensure compliance with regulatory requirements and Initech’s BSA Program, policies, and procedures.
* Independent Testing - This category refers to one of the four pillars of an effective AML Compliance Program and is intended to assess the adequacy of Initech’s independent testing pillar.

Applicable mitigating controls related to each risk factor were documented, assessed, and given a rating of Strong, Adequate, Weak, or N/A based on the definitions provided in the following table.

|  |  |
| --- | --- |
| **Control Strength** | **Definition** |
| Strong | A rating of “Strong” indicates the control environment appears to be safe and sound. As a result, the risk of non-compliance with regulatory requirements, not operating in line with policies and procedures, and/or lacking a significant control/having a significant control breakdown is considered low. Preventative and detective controls appear to be in place for all critical requirements and functioning effectively. |
| Adequate | A rating of “Adequate” indicates the control environment appears to be satisfactory. As a result, the risk of non-compliance with regulatory requirements, not operating in line with policies and procedures, and/or lacking a significant control/having a significant control breakdown is considered moderate. Preventative and detective controls appear to be in place for critical requirements, but minor control issues have been identified and are being addressed. |
| Weak | A rating of “Weak” indicates the control environment appears to be unsatisfactory. As a result, the risk of non-compliance with regulatory requirements, not operating in line with policies and procedures, and/or lacking a significant control/having a significant control breakdown is considered high. Preventative and detective controls do not appear to be in place for critical requirements and/or other control issues have been identified but have not been addressed or addressed adequately. |
| N/A | The control category is not applicable to the risk factor or category. |

The assessed strength ratings were assigned corresponding point values as follows: Strong=2, Adequate=1, and Weak=0. The ratings for the individual control categories associated to a specific risk factor were averaged to determine the overall strength of controls associated to that risk factor. The rating for all risk factors within a risk category were averaged to determine the strength of mitigating controls for the risk category as a whole. The ratings for each category were subsequently averaged to determine Initech’s overall strength of mitigating controls.

### Residual Risk

The residual risk is the overall risk remaining after factoring in the adequacy, appropriateness, and applicability of controls related to the risk factors identified. The residual risk for each risk factor was determined using the chart provided.

|  |  |  |
| --- | --- | --- |
| Inherent Risk | Mitigating Control | Residual Risk |
| High | Weak | High |
| High | Adequate | High |
| High | Strong | Medium |
| Medium | Weak | Medium |
| Medium | Adequate | Medium |
| Medium | Strong | Low |
| Low | Weak | Low |
| Low | Adequate | Low |
| Low | Strong | Low |

The residual risk ratings were assigned corresponding point values as follows: Low=1, Medium=2, and High=3. The ratings for the individual risk factors within a risk category were averaged to determine the residual risk rating for that risk category as a whole. The residual risk ratings for each category were subsequently averaged to determine Initech’s overall residual risk rating.

### Results

Initech has a ***High*** residual AML risk. The overall residual risk was ultimately determined by assessing the level of inherent risk present and the strength of corresponding mitigating controls. A summary of the assessed inherent risk, strength of mitigating controls, and resulting residual risk across the identified risk categories is provided below. Initech prepared and implemented a strong BSA Program and supporting policies in line with its business growth, the potential rapid rate of adoption for DASH, and the demands of a fluid regulatory environment. However, the elevated level of inherent risk associated with both Initech’s services and geographic location ultimately drove the overall residual risk. Based on the methodology used, it was determined a rating of *high* accurately reflects Initech’s residual risk.

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Category | Inherent Risk | Mitigating Controls | Residual Risk |
| Customers and Entities | Medium | Adequate | Medium |
| Products/Services | High | Adequate | High |
| Geographic Locations | High | Adequate | High |
| **Companywide** | **High** | **Adequate** | **High** |

# **ANALYSIS AND RESULTS BY RISK CATEGORY**

The analysis and results for inherent risk, strength of mitigating controls, and residual risk for each of the four (4) risk categories are detailed below.

## Customers and Entities

The results for the Customers and Entities category are summarized in the table below. The following key is applicable across all risk categories.

|  |  |
| --- | --- |
| Low / Strong |  |
| Medium / Adequate |  |
| High / Weak |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Customer and Entities | Inherent Risk | Mitigating Controls | Residual Risk |
| Customer Base - Foreign |  |  |  |
| Customer Base - Domestic |  |  |  |
| Customer Types |  |  |  |
| Change in Customer Base |  |  |  |
| **Overall Category** | **Medium** | **Adequate** | **Medium** |

### Inherent Risk

Initech’s overall inherent risk for Customers and Entities was deemed to be ***Medium***.

### *Customer Base - Foreign*

Initech anticipates a relatively small cohort of customers residing in foreign locations will initiate transactions via its kiosks. Initech based this determination on several factors. Firstly, Initech does not market its services outside the U.S. or have any foreign operating locations, thereby reducing exposure to customers residing in foreign locations. Secondly, the kiosks are not located at or near an international border crossing nor in or around a known international tourist area or destination. Further, Denver International Airport is located approximately 45 miles from Boulder, Colorado. Thirdly, the manufacturer configured the kiosks to accept only U.S. Dollars prior to Initech taking delivery. Thus, a prospective foreign customer must necessarily possess his/her non-native currency prior to initiating a transaction with an Initech kiosk. Therefore, it is believed few, if any, foreign residents or visitors will travel directly to or otherwise have occasion to patronize Initech kiosks. These considerations on balance result in a ***Medium*** inherent risk for this factor.

### *Customer Base - Domestic*

Initech estimates with limited exception that prospective kiosk customers transacting the purchase or sales of DASH will reside almost exclusively within a High Intensity Drug Trafficking Area (“HIDTA”). The kiosks themselves are physically located within a HIDTA, while several neighboring communities share the HIDTA designation. Separately, research determined that neither Initech kiosk is located in or around any High Intensity Financial Crime Area (“HIFCA”) nor domestic geographic location that might otherwise be labeled higher risk (e.g. Geographic Targeting Orders). This results in a ***High*** inherent risk for this factor.

### *Customer Types*

The FFIEC Exam Manual stipulates certain customers may pose an increased risk of money laundering or terrorist financing due to the nature of their business, occupation, or anticipated transactional activity.

Customer types that may pose an increased risk include, but are not limited to, the following:

* Foreign financial institutions including banks, money service providers, and currency exchanges
* Non-bank financial institutions such as money services businesses (MSBs), casinos, brokers/dealers in securities, and dealers in precious metals, stones, or jewelry
* Cash-intensive businesses such as convenience stores, restaurants, liquor stores, or privately owned ATMs
* Non-governmental organizations (NGOs) and charities
* Professional service providers such as attorneys, accountants, doctors, or real estate brokers.

Initech DASH kiosks are unconducive to non-individual (business/entity) users. Generally, it’s believed highly unlikely a business would utilize a DASH kiosk to initiate an exchange of U.S. Dollar-denominated currency for DASH-denominated cryptocurrency, and vice versa. Merchants accepting cash typically do not seek to exchange these funds for their cryptocurrency equivalent due to both currency volatility and the need to readily access capital for ordinary, everyday business expenditures. Further, in addition to logistical challenges, kiosks impose significantly higher fees than merchant platforms.

While its operating model is unconducive to non-individual users, the Initech kiosks may attract cash-intensive businesses seeking an alternative store of value in light of enhanced cash deposit controls and other de-risking activities common to traditional financial institutions. Although possible, the logistics of traveling to a stationary DASH kiosk for the exchange of business revenues, coupled with the cryptocurrency’s price volatility, suggest such an arrangement is highly unlikely, particularly on a recurring basis.

Separately, DASH kiosks are unfavorable to the high-volume speculative DASH trading, which regulators have cited as an ongoing area of concern. Such consumers would most likely seek platforms offering real-time trading, analytics, immediate order execution, price quotes, and other features common to professional traders.

In summary, the overwhelming majority of kiosk users are expected to be low or moderate risk customer types due to a combination of expected user attributes and the services offered. This results in a ***Low*** inherent risk for this factor.

### *Change in Customer Base*

Initech believes, based on its business model, the user profile of its kiosks will remain relatively consistent through the current Risk Assessment. Specifically, the physical, stationary kiosks will likely continue to attract individuals residing in close proximity who already possess a third-party DASH wallet app and a fundamental knowledge of cryptocurrency. Nevertheless, the rapid rate of DASH adoption among individuals, growth and innovation among DASH companies, and the fluid nature of the cryptocurrency ecosystem present the distinct possibility of a change in customer base. This results in a ***Medium*** inherent risk for this factor.

## Mitigating Controls

The strength of controls as it relates to Customers and Entities for each control category is provided below. The following key is applicable for mitigating controls across all categories.

|  |  |
| --- | --- |
| Low / Strong |  |
| Medium / Adequate |  |
| High / Weak |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Control Categories** | **Governance / Oversight** | **Policies / Procedures** | **Surveillance / Monitoring** | **Testing / Monitoring** | **Independent Testing** | **Combined Rating by Risk Factor** |
| Customer Base - Foreign |  |  |  |  | N/A |  |
| Customer Base - Domestic |  |  |  |  | N/A |  |
| Customer Types |  |  |  |  | N/A |  |
| Change in Customer Base |  |  | N/A | N/A | N/A |  |
| **Overall Rating for Customers and Entities** | | | | | | **Adequate** |

Initech’s overall strength of mitigating controls for Customers and Entities was assessed as ***Adequate***.

Key areas of strength that contributed to the overall rating include policies and procedures, surveillance and monitoring, and to a lesser extent, Initech’s operating model and business strategy. Appropriate policies and/or procedures are in place to address relevant BSA/AML topics related to customers, including a strong Know Your Customer (KYC)/Customer Due Diligence (CDD) Policy, and the review of customers for potentially suspicious activity via alert routines. The KYC/CDD Policy includes customer OFAC and other watchlist screening and standardizes the collection, recording, and verification of required information in line with, and in some instances exceeding, minimum regulatory requirements.

Separately, governance and oversight were generally viewed as adequate due to direct management engagement and oversight of BSA/AML responsibilities. Not unlike many startup or small-scale MS’s, Initech’s BSA Officer maintains additional employment roles with separate responsibilities. Understandably, this necessarily limits the time and resources that can be reasonably devoted to day-to-day compliance activities. Notwithstanding present management engagement, due to the delayed implementation of its formal AML Program, Initech elected to take a more conservative approach by assigning the “Adequate” rather than “Strong” strength of control for governance and oversight throughout the Risk Assessment.

Key areas of weakness that contributed to the overall rating include testing and monitoring across all control categories. Initech is actively preparing a system of periodic testing and monitoring for its KYC functionality and alert routines.

## Residual Risk

Initech has a***Medium*** residual AML risk for Customers and Entities. Although key weaknesses were identified relating specifically to testing and monitoring, the strength of the BSA Program, KYC/CDD Policy, and alert routines resulted in a *medium* residual risk for this category.

## Products/Services

The results for the Products/Services category are summarized in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Products/Services** | **Inherent Risk** | **Mitigating Controls** | **Residual Risk** |
| DASH Kiosks  DASH In – Cash Out |  |  |  |
| DASH Kiosks  Cash In – DASH Out |  |  |  |
| **Overall Category** | **High** | **Adequate** | **High** |

*Note*: Initech does not engage in nor offer any financial products. Its business model is limited to the provision of the above-referenced service offerings.

### Inherent Risk

Initech’s overall inherent risk for Services was deemed to be ***high***.

Regulatory guidance and the FFIEC Exam Manual identify certain services that pose an increased risk for money laundering and terrorist financing activities based on the nature of the services themselves. Services, for example, that allow for the rapid movement of funds, transactions involving foreign locations, user anonymity, the handling of high volumes of currency or currency equivalents, and new or nascent financial technologies are considered to be of higher risk.

### *DASH Kiosks, DASH In – Cash Out*

Initech offers digital-to-fiat currency exchange via its kiosks. This service facilitates the exchange of DASH-denominated cryptocurrency for U.S. Dollar-denominated cash, and thus involves potential anonymity or pseudo-anonymity of its users. DASH offers a degree of anonymity in the sense that a DASH address is not necessarily tied directly to a specific individual as with a traditional bank account and may be passed to a third-party without formal record. One person could potentially hold multiple addresses and, in theory, there would be no audit trail linking those addresses together or means of identifying ownership. Moreover, generally speaking, regulatory guidance deems new or emerging products, services, and/or transactional technologies as posing a heightened level of inherent risk.

### *DASH Kiosks, Cash In – DASH Out*

Initech offers fiat-to-digital currency exchange via its kiosks. This service facilitates the exchange of U.S. Dollar-denominated cash for DASH-denominated cryptocurrency. In addition to possessing the inherent risk properties documented within “DASH Kiosk, DASH In – Cash Out,” the accepting of cash poses an additional layer of risk. Cash remains the payment method of choice among illicit actors and, whether or not generated by criminal activities, is often used by criminals or those engaged in legally marginal activities as an instrument to disguise or obscure any potential financial audit trial.

### *Anticipated Transactional Activity*

The anticipated transactional volume and denominations (USD) on a monthly basis for the exchange of U.S. Dollar-denominated currency for DASH-denominated cryptocurrency, and the exchange of DASH-denominated cryptocurrency for U.S. Dollar-denominated currency are summarized below. The data reflects a mix of past transactional activities conducted at Initech kiosks and national and regional marketplace analysis conducted by members of Senior Management.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Monthly Activity | **Unidirectional kiosk** | | **Bidirectional kiosk** | |
| Volume and Transactional Amount | Volume | Aggregate Transaction  Amount ($) | Volume | Aggregate Transaction  Amount ($) |
| Currency Exchange / Monetary Instrument  DASH In – Cash Out | N/A | N/A | 9-12 | $2,655-$3,540 |
| Currency Exchange / Monetary Instrument  DASH Out – Cash In | 90-120 | $26,550-$35,400 | 81-108 | $23,895-$31,860 |
| **Total** | 90-120 | $26,550-$35,400 | 90-120 | $26,550-$35,400 |

Initech anticipates processing on average approximately 3-4 transactions per day, per kiosk, in the average transactional amount of $295.

Importantly, DASH industry research suggests that for most new DASH kiosks, transactional volume tends to begin very slowly for at least the first two to three months of operation until such time as the DASH community becomes aware and has occasion to patronize the new kiosks. As such, Initech may experience lower than anticipated transactional volumes for the bidirectional kiosk which has yet to be deployed, as detailed above.

### Mitigating Controls

The strength of controls as it relates to Services for each control category is provided below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Control Categories** | **Governance / Oversight** | **Policies / Procedures** | **Surveillance / Monitoring** | **Testing / Monitoring** | **Independent Testing** | **Combined Rating by Risk Factor** |
| DASH Kiosks  DASH In –  Cash Out |  |  |  |  | N/A |  |
| DASH Kiosks  DASH Out – Cash In |  |  |  |  | N/A |  |
| **Overall Rating for Services** | | | | | | **Adequate** |

Initech’s overall strength of mitigating controls for Services was assessed as ***Adequate***.

Fundamental controls in place around Initech’s high risk services were deemed to be strong and positively impacted the aggregate strength of mitigating controls. There were some weaknesses related to governance and oversight, much of which is the byproduct of an emerging startup and evolving organizational structure. Control weaknesses in testing and monitoring, which are currently being addressed, ultimately inhibited a stronger combined rating.

While Initech mandates employees complete a targeted BSA training program as a condition of continued employment, independence and stronger reporting lines will necessarily evolve as the business matures from its current startup status. This resulted in an *adequate* rating for Governance/Oversight.

An appropriate BSA Program and strong KYC/CDD Policy, including OFAC and other watchlist screening, effectively address relevant activities associated with Initech’s services. This includes the identification, recording, and retention of transactions by threshold in accordance with Currency Exchange and Monetary Instrument Log requirements. The combination of KYC/CDD Policy and watchlist screening resulted in a *strong* rating for Policies/Procedures.”

Initech’s alert routines are designed to detect, review, and escalate potentially suspicious activity. Routines in place include both dollar and volume thresholds, and incorporate parameters for identifying money movement, structuring, and CTR reportable events, as applicable. This resulted in a *strong* rating for Surveillance/Monitoring.

The surveillance and monitoring models, though deemed adequate and robust, are not yet subject to testing and monitoring, as previously acknowledged. In the interim, Senior Management has access to detailed transactional reports via kiosk manufacturer-provided software, which may facilitate more fluid adjustments to alert routines. However, the absence of a formal system at this time resulted in a *weak* rating for Testing/Monitoring.

### Residual Risk

Initech has a ***High*** residual risk for Services. Although areas of strength were identified – including the BSA Program, KYC/CDD Policy, alert routines, and targeted training – key weaknesses ultimately drove this rating. The absence of a formal system for testing and monitoring transactional activities, coupled with governance/oversight limitations and the risks associated with customer-initiated cash transactions, resulted in a *high* residual risk for this category.

## Geographic Locations

The results for the Geographic Locations category are summarized in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Geographic Locations** | **Inherent Risk** | **Mitigating Controls** | **Residual Risk** |
| Operating Locations - Domestic | N/A | N/A | N/A |
| Operating Locations - Foreign | N/A | N/A | N/A |
| Transacting Locations - Domestic |  |  |  |
| Transacting Locations - Foreign | N/A | N/A | N/A |
| **Overall Category** | **High** | **Adequate** | **High** |

### Inherent Risk

Initech’s overall inherent risk for Geographic Locations was deemed to be ***high***.

The FFIEC Exam Manual speaks specifically to both foreign and domestic locations that present an increased level of AML risk. These include, but are not limited to, the following:

* Countries subject to OFAC and other watchlist sanctions
* Jurisdictions of primary money laundering concern as determined by the Secretary of the Treasury and those subject to special measures imposed by the Secretary of the Treasury
* Jurisdictions identified by the Financial Action Task Force on Money Laundering (FATF) as having deficiencies regarding combating money laundering and terrorist financing
* Countries and jurisdictions identified in the U.S. Department of State’s annual International Narcotics Control Strategy Report (INCSR) as jurisdictions of primary concern
* Offshore financial centers
* High Intensity Drug Trafficking Areas (HIDTAs)
* High Intensity Financial Crime Areas (HIFCAs).

Initech kiosks operate and facilitate transactions exclusively within designated HIDTAs. As previously acknowledged, Initech kiosks are physically located within a HIDTA, while several neighboring communities have also been designated HIDTAs. The Rocky Mountain HIDTA (“RMHIDTA”) comprising the individual HIDTAs within Colorado, Utah, and Wyoming, determined that its well-established infrastructure and the region's central location within the United States make the area conducive to illegal drug transportation and distribution. Additionally, RMHIDTA determined that state-level marijuana legalization in Colorado has led to an increase in interdiction seizure destined for other parts of the country. In September 2016, RMHIDTA issued a report entitled “Legalization of Marijuana in Colorado: The Impact.” Among the findings, RMHIDTA determined the following based on state highway patrol traffic stops: (1) during 2009–2012, when medical marijuana was commercialized, the yearly average number interdiction seizures of Colorado marijuana increased 357% from 53 to 242 per year; (2) highway patrol interdiction seizures of Colorado marijuana increased 37% from 288 to 394 during 2013–2015, when recreational marijuana was legalized; and, (3) the total average number of pounds of Colorado marijuana seized from 2005– 2008 compared to 2009–2015 increased 30% from 2,763 pounds to 3,586 pounds. The concentration of HIDTAs, coupled with the ramifications of strong state-level marijuana legalization, results in a *high* inherent risk for domestic transacting location.

As it pertains to operations, Initech does not maintain any foreign locations. Additionally, Initech does not offer any transactions in, to, or from foreign countries. Separately, while its operating center or headquarters is located in Boulder, Colorado, Initech’s services are facilitated via its kiosks. Consequently, neither domestic nor foreign operating locations were applicable to this Risk Assessment.

### Mitigating Controls

The strength of controls as it relates to Geographic Locations for each control category is provided below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Control Categories** | **Governance / Oversight** | **Policies / Procedures** | **Surveillance / Monitoring** | **Testing / Monitoring** | **Independent Testing** | **Combined Rating by Risk Factor** |
| Operating Locations - Domestic | N/A | N/A | N/A | N/A | N/A | N/A |
| Operating Locations - Foreign | N/A | N/A | N/A | N/A | N/A | N/A |
| Transacting Locations - Domestic |  |  |  |  | N/A |  |
| Transacting Locations - Foreign | N/A | N/A | N/A | N/A | N/A | N/A |
| **Overall Rating for Geographic Locations** | | | | | | **Adequate** |

The overall strength of mitigating controls was deemed to be ***Adequate***.

The same key controls apply here as those considered in the Services section, including policies and procedures, surveillance and monitoring, and targeted training. Appropriate policies and procedures exist to address relevant BSA/AML topics related to activities associated with Initech’s service offerings. These include the identification of cash activity that may require CTR filing; the Currency Exchange Rule; Monetary Instrument Log; recordkeeping requirements; and the detection, review, and/or escalation of potentially suspicious activity.

An appropriate BSA Program and strong KYC/CDD Policy, including OFAC and other watchlist screening, effectively address relevant activities associated with Initech’s service. This includes the identification, recording, and retention of customer information and transactions by threshold in accordance with Currency Exchange and Monetary Instrument Log requirements.

Initech’s alert routines are designed to detect, review, and escalate potentially suspicious activity. Routines in place include both dollar and volume thresholds and incorporate parameters for identifying money movement, structuring, and CTR reportable events, as applicable.

The surveillance and monitoring alerts, though deemed adequate and robust, are not yet subject to testing and monitoring, as previously acknowledged. In the interim, Senior Management has access to detailed transactional reports, via kiosk manufacturer-provided software, which may facilitate timely examination and more fluid adjustments to alert routines.

Further opportunities for improvement include governance and oversight controls. While Initech mandates employees complete a targeted BSA training program as a condition of continued employment, independence and stronger reporting lines will necessarily evolve as the business matures from its startup status.

### Residual Risk

Initech has a ***High*** residual risk for Geographic Locations. While Initech has adopted robust mitigating controls, the absence of formal testing coupled with an elevated level of inherent risk associated with its transactional geographic locations resulted in a *high* residual risk for this category.

# **TRENDING AND DIRECTION OF RISK**

Although it is not expected there will be changes in Initech’s BSA risk profile as it relates to the overall composition of its customer base or services offered, the anticipated business growth of Initech will by nature increase its inherent risk, particularly as it relates to incorporating newer locations and the ensuing increase in aggregate transactional volume. Further, Initech anticipates greater awareness of DASH and digital currencies in general will yield an increased rate of adoption among consumers. In line with this growth, Initech anticipates and is committed to improving and strengthening mitigating controls, including implementation of independent testing. This will serve Initech well, as regulatory expectations have increased in recent years, especially among MSBs, and it is expected this upward trend will continue forward.

While Initech designed its BSA/AML strategy to scale and adapt to future business growth, as previously referenced, any future material changes (e.g., additional kiosks or new service offerings) will necessitate revision of the Risk Assessment.

# **RECOMMENDATIONS**

Recommendations as it pertains to each risk category are described in detail below.

## Customers and Entities

Initech anticipates and has prepared for incremental customer growth among its kiosks. Over time, increased users will result in more alert routines and greater outlay of overall compliance resources. Further, entry into new markets, while examined within this Risk Assessment, inherently pose new and sometimes unforeseen issues. Continued expansion, coupled with increased regulatory requirements and expectations regarding KYC/CDD, may result in an increase in risk for regulatory non-compliance. Initech is encouraged to carefully consider the potential effects of growing and altering its existing customer base prior to any further expansion. Continuing to address the implementation of testing and monitoring will serve to strengthen and solidify its KYC/CDD capabilities, and better prepare Initech to address any changes to its customer base.

## Products/Services

While Initech’s services were determined to be high risk, fundamental controls including a robust BSA Program, KYC/CDD Policy, and alert routines were deemed strong. Overall, Initech took a conservative approach to its controls, anticipating a growing customer base, increasing regulatory requirements, and escalating rate of DASH adoption. Further, Initech is encouraged to continue utilizing blockchain explorer data and other emerging tools to research customers and customer transactional activities as part of its ongoing KYC/CDD efforts.

Separately, while management has access to detailed transactional reports, there is currently no formal testing and monitoring in place to ensure optimal alert routines and the ongoing adherence to various reporting requirements. Initech is encouraged to continue developing a testing and monitoring policy, which it has already begun to pursue. Such testing and monitoring is all the more necessary given its multiple kiosk footprint, and the overall increasing rate of DASH adoption.

## Geographic Locations

While Initech does not currently have formal plans to expand the geographic footprint of its kiosk operation beyond greater Denver, Colorado, the company remains open to the possibility in the future. Prior to any planned expansion, it is imperative that Initech individually assess and analyze the geographic risk (e.g. HIDTA, HIFCA, GTO jurisdictions) with any new potential location. At present, Initech kiosks are located within or among HIDTAs, which will continue to necessitate the utmost commitment to its BSA Program, KYC/CDD Policy, and alert routines. Separately, expansion into other states outside of Colorado will require research to determine if licensure is necessary or under what circumstances it may be required.

Notwithstanding strong existing controls, Initech is encouraged to continue addressing the implementation of testing and monitoring. This will serve to enhance the tuning of alert routines and prepare Initech for any future expansion.

# **SENIOR MANAGER APPROVAL**

Initech’s Risk Assessment must be approved in writing by a member of Senior Management.

Senior Management has approved this Risk Assessment in writing as reasonably assessing Initech’s inherent risks, mitigating controls, and residual risks. This approval is indicated by the signature on the following page.

Signed:

Name:

Title:

Date:

1. At present, the Board of Directors of Initech consists of the Managing Member. [↑](#footnote-ref-1)