

**

Business Plan

## Executive Summary

### Product

Microsoft 365 Reseller and Managed Service Provider for Risk Management (Risk Management as a Service).

NIST Assist is a Microsoft Silver Partner and License Reseller, providing Multi-Partner Products and Services packaged / bundled with Risk Management as a Service. Products include:

* Microsoft Azure
* Microsoft 365 Licenses
* Risk Management Services
* Professional Services from Help Desk to Executive Thought Leadership
* White label products and services



### Customers

NIST Assist serves small to medium size companies, primarily in the government contracting sector, and customers in various supply chains who have security and compliance requirements regulated by an agency or industry association. Increasing markets are opening up due to increased governmental requirements such as CMMC, and heighted states of awareness regarding security and compliance in general. NIST Assist has also generalized and templatized risk management as a service for the general market in response to market expansion opportunities.

Differentiating components that are key to future growth center on a two-factor approach of (1) muti-partner relationships we apply to our customer eco system to address the customers key risk areas, and (2) the application of the NIST standards that focus on security and compliance controls that reduce risk and increase efficiencies of the customer through standardization and corporate maturity. Our customer engagement model has a feedback loop of recuring risk management meetings with each customer, this allows NIST Assist to pick and chose which areas of improvement are most profitable to take on internally, and those that are best served through strategic alignment of specialized service providers. For example, we identify backup as a risk, and resell backup services to the customer. On the other hand, a customer who needs a custom app solution is more likely to choose to have us create one for them as their trusted technology partner.

## Company Description

### Mission Statement

NIST Assist is dedicated to supporting organizations in adopting standards and practices through systematic incremental improvements. Our mission is to assist customers in identifying and navigating their unique roadmap to success. We are committed in this endeavor to the foundational principles of confidentiality, integrity, and availability.

### Principal Members

Scott Parramore – Founder of the NIST Assistance Program in the Microsoft Partner Network

Don Griggs – Co-Founder of AIIM Technologies, and predecessor to NIST Assist

Shouvik B. – Business Partner with NIST Assist Teaming Agreements

### Legal Structure

Readypool Technical Services DBA NIST Assist is a sole proprietor established in 2013.

NIST Assist llc. has been established since 2021.

Bank of America Business Account since 2013 (still in DBA).

NIST Assist llc. has Teaming Agreement with B12 and has several contracts in various states of execution at any given time. This agreement provides the NIST Assistance program to its clientele as a white label service.

## Market Research

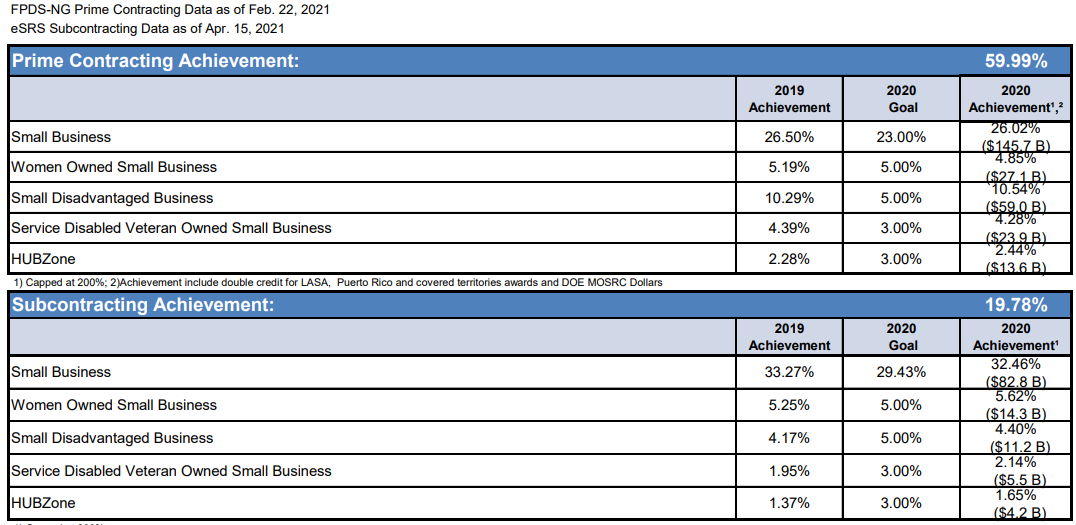
### Industry

In general, the “Risk Management as a Service” concept can be applied to any industry, but has its largest footprint in the government contracting sector (where NIST Assist started) because security and compliance are foundational components of a risk management framework. NIST Assist has an established reputation in this market as a Microsoft Silver Partner for over a decade. Over this decade we found that talking about risk management and increased efficiency was more attractive than cybersecurity and compliance, so we changed from Readypool Technical Services to NIST Assist in 2017.

**Government Space**

We now serve 2 markets, first and foremost is the government contracting sector where we began. To understand the opportunity here, it is important to understand how the market is changing over the next few years, and how we are positioned to evolve with it. Over the past 3 years the government has been developing and implementing a set of security standards that are to be mandated for all government supply chain contracts, including all small business contracts and third-party relationships of those contracts. From 2017, most government contractors and subcontractors had to complete a System Security Plan (SSP) and a Plan of Actions & Milestones (POA&M) for assessment of their cybersecurity stance according to the NIST 800-171 standard. This standard comprises 110 controls and requires analysis of a subcontractor’s response to cybersecurity needs and implementation outcomes. However, by 2019, the government realized that neither government acquisition officers nor those working for prime contractors, or subcontractors responded adequately to the regulations. For this reason, with Congressional approval, the DoD commissioned updated regulations and standards known as the Cybersecurity Maturity Model Certification (CMMC), which are now mandatory for all DoD contracts from September 2020, and will be pushed out to all government contracts over the next few years.

Previously contractors had the responsibility for the implementation, monitoring, and certification of the integrity of their IT systems and the sensitive information that these systems generated, stored, or transmitted. Although contractors are still responsible for ensuring the implementation of essential cybersecurity measures, the CMMC alters this paradigm. It requires a third-party assessment of compliance with procedures, capabilities, and specific mandatory requirements to help them adapt to new cyber threats from adversaries of the US. The market potential for this industry is based on the amount of small business contract awards, and for context we have provided the latest 2020 report here:



With over $200B being awarded to prime contractors, and $100B to subcontractors, we estimate this market will be underserved for at least 3 years because there is a shortage of providers, and only limited number of certified professionals. Market research and interviews with current contractors in the business indicate a low profit margin associated with this type of contract work in the short term. The key takeaway here however is not the immediate sales profit opportunity, but the fact that we become their trusted advisor. In our experience the long-term strategy pays dividends in trust.

While recuring revenue accounts for about 20% of our income, assessments account for about 30% of business. Currently NIST Assist performs pre-check assessments and preparation services to many of its clients. However, NIST Assist will be seeking to become a CMMC Third Party Assessor Organization, or C3PAO, which is an organization authorized by the CMMC-AB to conduct, and deliver CMMC assessments.

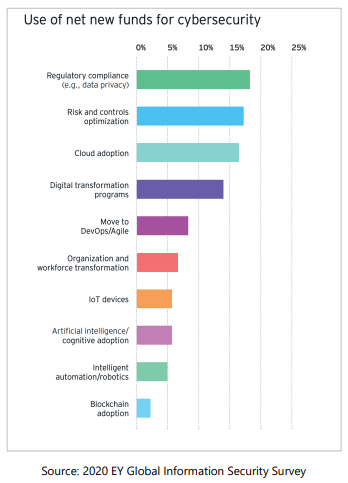
A company cannot do both the assessment and the certification by law. Assessments, which make up the bulk of work being performed now, are relatively small gigs that average $5K to $10K and take 4 weeks. A certification however averages more than $70K and takes several months. In several years, pre-assessments will no longer be the bulk of work as they are today prior to the CMMC transition. Our strategy is to partner with a C3PAO in a mentor / mentee arrangement, as is customary, and thus transition to a certification authority within 2 years. This extends our current market, and opens up whole new markets in this sector.

**SMB Commercial Services**

This market is referred to as a Microsoft CSP, or the Cloud Solution Provider (CSP) Program. To understand this market some history will give context to the importance of our position and status within the Microsoft Partner Network. NIST Assist, formerly Readypool Technical Services, became a Microsoft CSP Partner when the program was first launched in 2013. At that time, it was open to anyone who had a Microsoft Certification, and had very little requirements because Microsoft was transitioning from a traditional sales organization to a service provider and needed partners to supplant the traditional sales department. The Partner Network replaced traditional sales with certified Microsoft resellers who now number in the thousands. Today, however, due to the increased requirements, becoming a Microsoft CSP requires a minimum investment in excess of $1M.

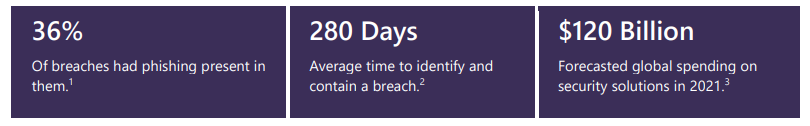
The current Microsoft CSP landscape for businesses can accurately be described in one word: complicated. More numerous and advanced threats, more nebulous and complex compliance requirements, more difficult and intricate infrastructure to secure. Simply put, keeping data, workloads, and users secure is more than a full-time job—and organizations are having trouble keeping up. The graphic below illustrates the myriad offerings and postures taken by security companies, highlighting the fragmented nature of the market. However, this harsh environment represents a significant opportunity for partners looking to offer security as a managed service.



For even the most adept IT and incident response teams, effectively handling patching, malware threats, and intrusion detection can be too difficult to manage without help. Managed Service Providers can offer services to ensure enterprise clients are secured. But in this age where new security breaches surface in the news almost daily, how can partners help customers stay ahead of the game, and avoid becoming a statistic?

According to the Microsoft Digital Defense Report 2020, attacks have become more sophisticated, and ransomware was the most common reason for incident responses from October 2019 to July 2020. Microsoft blocked more than 13 billion suspicious emails, and more than a billion of those used URLs set up to launch phishing credential attacks. And the first half of 2020 saw a 35% increase in IoT attacks compared to the second half of 2019.

According to the 2020 IBM Cost of a Data Breach Report, the cost incurred for each lost or stolen record of sensitive data is now at $150, with the total consolidated cost of a data breach at $3.86 million. Meanwhile, according to the PWC Global State of Information Security Survey, the sources of security incidents perpetrated by current employees remains high, and that from business partners continues to rise. Additionally, many CISOs feel the most challenging thing is to secure the budget they need to provide the levels of cybersecurity they desire, according to the EY Global Information Security Survey. All of this combines to create the demand for partners to improve their customers defense with information protection. Source: 2020 EY Global Information Security Survey According to the Verizon 2021 Data Breach Investigations Report, organizations surveyed saw phishing as the top threat. Additionally, these organizations identified zero-day attacks and targeted cyber-attacks to steal financial information, disrupt or deface the organization, or steal intellectual property or data. Yet, according to the EY Global Information Security Survey, only 26% of breaches from these threats in the last 12 months were detected by the SOC. In today’s world, it’s clear that increasing trust and managing security, compliance and identity is a struggle for many organizations. But as Microsoft’s Digital Defense Report points out, actors have continued to evolve their attack techniques making the importance of improving security comprehensively has become even more evident:

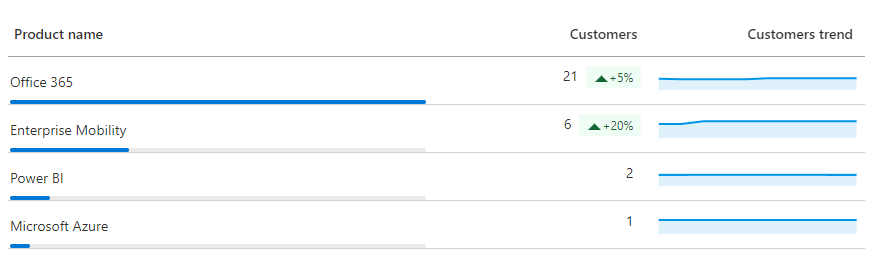


A recent study by Microsoft research shows that 93% of Chief Information Security Officers (CISOs) and Data Protection Officers are concerned with insider risk. In addition, 66% stated they were “very concerned”. Insider threats are reportedly the primary cause for over 60% of data breaches and percentage is increasing. Last year we saw a former employee at Amazon charged with insider trading by having access to sensitive financial data and sharing with family members, there was an unsuccessful attempt to bribe to a Tesla employee with $1 million in exchange for installing malware in the system, and an incident with “two rogue” employees resulted in Shopify’s stock price to drop 1.2%.

NIST Assist has partnered with Microsoft because they are the predominant player in this industry and market and have the best program of assistance and alignment to our market. We will use the Microsoft Partner Network Benefits and accompanying market research and playbooks to grow the commercial business.

### Detailed Description of Customers

The target customers as of today are primarily government contractors. These customers generally have between 15 to 300 users. Currently we have 21 Microsoft 365 customers, 6 Enterprise Mobility, 2 PowerBI, and 1 Azure;



**Total users currently supported: Approximately 985**

**Capacity: 1200**

Additional customer targets include establishing what we call *prime contractor eco-systems*. Prime contractors have requirements to use small businesses, and there is a common security and compliance watermark they must adhere to within their supply chain. NIST Assist provides the prime-contractors with white labeled security and compliance services that are applied to the sub-contractors on behalf of the prime-contractor. Sub-contractors are generally small to medium size companies who are in a mentor/mentee program with a prime contractor, and are generally not prepared to navigate the public sector requirements. NIST Assist has established one relationship of this nature and has standardized the approach and solution package.

### Company Advantages

The overall company advantage is the Risk Management approach. Customers pay us a recuring subscription fee to help ensure they are secure and compliant with the appropriate levels of risk management for their organization. This is done through regularly scheduled risk management meetings. The results of these meetings have only 3 potential outcomes:

1. The customer will be required to perform some activity, and will have to make a choice about how to address a risk. We discuss the options, and determine if outsourcing is viable. History shows that customers will outsource everything they do not have to do if they can justify the cost. The advantage here is the customer often does not have the skill or desire to perform the task.
2. NIST Assist will perform a task order: A Risk Management Master Agreement is used as a vehicle to charge one off projects to the customer as a monthly line item. The advantage here is that we are the only ones qualified to perform the task, and in many cases there is an upsell opportunity.
3. NIST Assist will engage one of its approved partners to provide a product or service: We continue to grow reseller relationships with key partners who can provide ancillary services through a white label or teaming agreement.

Significant advantage is also gained by the founders 20 years of experience in this sector, and unique insights into teaching the fundamental principles of the trade craft to staff. By developing systems that enable our knowledge workers to manage customer maturity, we can effectively scale operations. As a small firm we spent years forging deep relationships and developing partnerships that have given us invaluable awareness of how companies successfully navigate through the 5 stages of maturity. The following highlights these advantages;

* As a Microsoft Partner our biggest advantage is the Partner Resources and Benefits that help bring solutions to market within the Microsoft Eco System. This is much like a franchise in that there are requirements and quotas that qualify partners for additional resources and benefits. The benefits are too numerous to list here but can be presented.
* We have people who answer the phone. We formulate a tight relationship with stakeholders / end users and become a trusted advisor. Customers can pick up a phone and get an answer right away, this has become a differentiator and customers love this aspect of our assistance. Our personal white glove service and human touch are well received and highly valued in risk management; our customers trust us because we are in a high trust role.
* Well documented, systematic, and transparent approach (using many of the Partner resources and benefits) translates to measurable results and dashboards that are built into the platform. The advantage here is that we do not have to maintain or support much of the technology we are using, it is part of the platform and considered a benefit to us from Microsoft.
* Highly experienced core staff have been trained for over 1 year in each category of corporate maturity. They have had hands on experience and real world application of the cybersecurity maturity model. They have been trained from day one on the core principles of this business plan, and are prepared in their trade craft to train the trainer and scale operations using the “2 in a box” approach.

### Regulations

NIST Assist must maintain a security and compliance watermark that is commensurate with its customers. As a Managed Service provider with a trust relationship we are considered an insider threat by definition and must maintain at a minimum the standards and practices as outlined in NIST Special Publications 800-171, DFAR 7022, and ISO 27001. In virtually all engagements our customers are onboarded with very low scores and high risk scenarios, and once we become the Digital Partner of Record, we have additional requirements and regulations from Microsoft that include Anti-Trust Training and Awareness and other requirements based on Duty of Care.

Regulations are a key factor in our business model. NIST Assist subscribes to multiple industry resources and has established services that alert us to changes in regulatory requirements.

## Service Line

### Product/Service

#### Managed Services Include:

* Azure / Microsoft Products and Services centered on Microsoft 365
* Business Process Reengineering Analysis
* On-Site Office Management Services
* Business Process Reengineering
* Operations Improvement
* Risk Management / RMaaS

#### Revenue Streams:

* Microsoft / Azure / AWS License reseller - monthly recuring revenue
* Third party products and services - other income / internal user rights
* Managed Services / monthly recurring revenue
* Task orders and projects / time and material & fixed cost revenue
* Teaming agreements / white label monthly income

### Pricing Structure

TBD:

* Principal, $150
* Account Executive, $140
* Project Manager, $135
* Project Coordinator, $100
* Business Analyst, $90
* Process Analyst, $90
* Financial Analyst, $85
* Technologist, $75

### Product Lifecycle

Customer / product lifecycle begins with an initial questionnaire that gives us situational awareness into the organization and gauges its maturity level. Once a subscription level is agreed upon, the customer is onboarded accordingly and where applicable becomes a Digital Partner of Record. The Digital Partnership is the vehicle upon which we transact with the provider on the customers behalf, and gives us an administrative role in the customers online tenant. All customers will eventually have an online tenant in Microsoft, Google, or AWS (or some hybrid). We primarily focus on Microsoft at this stage of growth, but some new customers may not migrate until their renewal date if applicable, so our lifecycle supports customers who are muti-tenant and in flux.

Once the administrative role is established through the DPOR, we perform an assessment, most often based on NIST 800-171 because it is the basis for most frameworks.

The outcome of the assessment is a list of immediate threats, corrective actions, and recommended activities that are presented as opportunities for improvement to the customer.

NIST Assist meets with its customers on a regular basis to discuss the most cost-effective way we can address their opportunities for improvement in order of priority.

The initial revenue stream begins with the subscription for risk management and has 1-3 year term pricing options. The second revenue stream begins when we start providing the licenses for the online tenant, which also carries 1-3 year terms, but are not coterminous with managed services, they are separate agreements. These 2 primary monthly recurring revenue streams apply to virtually all customers.

Other recurring revenue streams from partnerships may not apply in all cases and vary according to the agreement, provider, and other limitations.

### Intellectual Property Rights

Registered Domains include:

* Nistassist.com
* Readytechservices.com

The bulk of our intellectual property exists in the form of systems and content that includes customized SharePoint, PowerApps, and other software that has been developed over the past 10 years. This includes:

* Advanced research into threat vectors and risk mitigation techniques.
* Development of core principles of risk management – the NIST Assist approach (moving from a reactive state to a proactive state through standardization and optimization).
* Program Management Information System (PMIS) software and database architecture.
* Industry standard database structures for over a dozen industry types, like canine for example. These database schemas are invaluable to developing secure applications.
* Hundreds of articles, manuals, polices and procedures that have been customized and curated specifically for risk management, cross referenced with all relevant regulations, and categorized using content management.
* Policy and procedure templates, SharePoint templates, PowerApps templates, and a host of primers that have been developed to jump start many of the processes we do repeatedly.
* Detailed process flow charts for all business processes done in BPMN 2.0.
* Custom line of business applications like ticket tracker, Atera, and Compliance Manager.
* Advanced knowledge and documentation / experience regarding the application of Secure Score, Compliance Manager, MS Security and Compliance tools, Cloud App Security tools and the Defender Platform.
* Custom written “white hat” hacking tools that include port sniffers and IP trackers that identify bad actors on a network.
* Complete franchise platform and software package for white label, allowing us to scale multiple offices.
* Lessons learned and knowledgebase of risk management frameworks.
* Weapons accountability software (precursor to block chain).
* Advanced algorithms for iterating through records and monitoring / migrating data.

### Research and Development

Research has shown that effective risk management can bring a number of benefits to a business. Some of these include:

* Improved financial performance: By identifying and managing potential risks, a business can reduce its exposure to loss and improve its financial performance. This can lead to increased revenue, higher profits, and a stronger bottom line.
* Better decision making: Risk management helps businesses make more informed decisions by providing a clear understanding of the potential impact of different actions and decisions. This can lead to more effective and efficient use of resources, as well as improved strategic planning.
* Enhanced reputation: Effective risk management can help protect a business's reputation by preventing or quickly responding to potential crises. This can help maintain customer trust and loyalty, as well as attract new customers and partners.
* Compliance with regulations: Many businesses are subject to a wide range of regulations and standards, such as HIPAA, SOC2 and ISO 27001, that require them to implement specific controls and procedures to protect against certain types of risks. Risk management can help businesses ensure compliance with these regulations and avoid costly fines and penalties.
* Improved operational efficiency: By identifying and managing potential risks, businesses can reduce disruptions to their operations, increase productivity, and improve overall efficiency.
* Advanced Program Management Information System (PMIS) capabilities have been developed over the past 20 years, including in depth understanding of how this platform has evolved through the National Institute of Standards and Technology.

Overall, risk management is a vital component of any business's operations, providing a framework for identifying, assessing, and managing potential risks, and can bring a significant value to the company by improving its overall performance and resilience.

## Marketing & Sales

### Growth Strategy

There are several growth strategies NIST Assist has begun to use to expand its risk management offerings. Some of the most common include:

1. Market penetration: The company can focus on increasing market share within its existing markets by promoting its services to new customers and encouraging current customers to use more of its services.
2. Product development: We have developed new risk management services and added new features to existing services to appeal to new customer segments and address new types of risks.
3. Diversification: The company could expand into new markets or industries by offering its services to new types of customers. This could include expanding into new geographic regions or entering new industries such as healthcare, retail, or finance.
4. Mergers and acquisitions: The company could acquire other companies that offer complementary risk management services to quickly expand its offerings and gain access to new customers and markets.
5. Strategic partnerships: The company could form partnerships with other companies, such as technology providers, consulting firms, or insurance companies, to offer a more comprehensive range of services to customers and expand its reach.
6. Investing in technology: The company could invest in technology to automate and streamline processes and make it more efficient in providing the services. This also opens opportunities to offer new services such as AI-based analytics, automation and visualization of data.

Ultimately, the growth strategy a company chooses will depend on its specific goals, resources, and competitive environment. It may use a combination of these strategies to achieve its desired growth.

### Communicate with the Customer

Communicate with its customers is a key part of our strategy and is performed in a variety of ways to ensure that risks are effectively identified, prioritized, and managed. Some key communication methods we practice include:

1. Regular meetings: We hold regular risk management meetings with customers to review and update the risk register and discuss any new or emerging risks. During these meetings, we prioritize the remediation of risks based on their likelihood and impact, and develop a plan of action to address them.
2. Reports and documentation: We provide customers with regular reports and documentation outlining the risks identified and the actions being taken to address them. These reports are tailored to meet the customer's specific needs and are used to track progress and measure the effectiveness of the risk management program.
3. Communication platforms: We use a range of communication platforms such as email, telephone and video conferencing to keep in touch with customers and provide updates on the status of risk management activities.
4. Continuous improvement: We promote efficiency through continuous improvement by regularly reviewing and refining customers’ risk management processes and procedures. This helps to ensure that the program is always up-to-date and responsive to changes in the customer's business and the risk environment.
5. Mentoring: We provide mentoring and guidance to customers to help them develop the skills and knowledge needed to effectively manage risks on their own. This includes training on industry regulations and best practices, as well as coaching on how to use the risk management tools and techniques provided by the us.

Overall, effective communication is key to the success of any risk management program. By keeping customers informed and involved throughout the process, we can build trust, ensure that risks are effectively managed, and promote efficiency through continuous improvement and mentoring.

### How to Sell

Sell strategies have begun, or are planned to sell to existing and potential customers:

1. Networking and Referral: We currently rely on networking and referrals to build relationships with potential customers. This includes attending industry events, joining professional organizations, and building a strong relationship with customers to gain referrals. Currently this is the only way we have gained new customers, we have not done any marketing or engaged in a sales strategy.
2. Cold Calling and Emailing: The company could use cold calling and emailing to reach out to potential customers and introduce its services. This would typically involve researching potential customers and targeting them with personalized messages that highlight the benefits of the company's services.
3. Case Studies and Testimonials: We have used case studies and testimonials to showcase the effectiveness of our services and demonstrate the value it can provide to potential customers. These materials are used to demonstrate the company's expertise in past performance, and the success stories of the previous clients.
4. Proposal and Presentation: We have prepared proposals and presentations that outline our services, pricing, and how it can help the customer manage risks effectively. This has been effective to convince potential customers that the company's services are the best fit for their business.
5. Online marketing: The company could use online marketing strategies to reach potential customers such as SEO, PPC, and social media marketing. This would help the company to build brand awareness and generate leads.
6. Partnership: We have several partnership opportunities with other companies that offer complementary services.

Ultimately, the most effective sales strategy will depend on the company's target market, services offered, and resources. The company may use a combination of these strategies to reach and win new clients.