

PAYMENT INTEGRITY

***Public-Private Partnerships and the
Payment Integrity Research and
Analysis Capability Concept:
Methodology for Analyzing Owner and
Operator Alternatives***

November 2017

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release: 17-4135. Distribution Unlimited.

©2017 The MITRE Corporation. All rights reserved.

MITRE

Acknowledgments

The MITRE Corporation—a private, not-for-profit organization—operates federally funded research and development centers (FFRDCs), unique organizations sponsored by government agencies to assist with research and development, study and analysis, and/or systems engineering and integration. MITRE operates seven FFRDCs sponsored by the federal government. These are:

- National Security Engineering Center sponsored by the Department of Defense,
- Center for Advanced Aviation System Development sponsored by the Federal Aviation Administration,
- Center for Enterprise Modernization sponsored by the Department of the Treasury and co-sponsored by the Department of Veterans Affairs,
- CMS Alliance to Modernize Healthcare sponsored by the Centers for Medicare & Medicaid Services,
- The Homeland Security Systems Engineering and Development Institute sponsored by the Department of Homeland Security,
- Judiciary Engineering and Modernization Center sponsored by the Administrative Office of the U.S. Courts, and
- National Cybersecurity Federally Funded Research and Development Center sponsored by the National Institute of Standards and Technology.

MITRE also maintains a broad, independent research program, designed to explore emerging issues and potential solutions to benefit our government sponsors, industry and the public.

MITRE Study Team

Gary Ingber

Gordon Milbourn

Ted Sienknecht

Table of Contents

- 1 Introduction..... 1
 - 1.1 Purposes of Report..... 1
 - 1.2 Origin and Approach..... 1
- 2 Overview of Public-Private Partnerships and the Payment Integrity Research and Analysis Capability Concept 2
 - 2.1 Public-Private Partnerships..... 2
 - 2.2 The PIRAC Concept..... 4
 - 2.2.1 Mission 4
 - 2.2.2 Vision 4
 - 2.2.3 Key Operational Concepts..... 5
- 3 Methodology for Assessing PIRAC Owner and Operator Alternatives 8
 - 3.1 Background Research..... 8
 - 3.2 PIRAC Owner and Operator Definitions..... 8
 - 3.3 Alternatives Considered..... 9
 - 3.4 Evaluation Criteria 9
 - 3.5 Rating Scale and Weighting..... 11
- 4 Key Takeaways 14

List of Figures

- Figure 2-1. When to Consider a PPP 2
- Figure 2-2. Illustration of Left of Check Concept 5
- Figure 2-3. High-Level Overview of a PIRAC..... 6
- Figure 3-1. PIRAC Roles 9

List of Tables

- Table 3-1. Evaluation Criteria 10
- Table 3-2. Scoring PIRAC Owner 12
- Table 3-3. Scoring PIRAC Operator 12

1 Introduction

1.1 Purposes of Report

This report describes the relationship between Public-Private Partnerships (PPP) and the Payment Integrity¹ Research and Analysis Capability (PIRAC) concept, and describes a methodology for analyzing the Owner and Operator alternatives for a PIRAC. The use of PPPs and the PIRAC concept were key recommendations of the government-wide Payment Integrity study² conducted by The MITRE Corporation (MITRE), a not-for-profit organization that operates federally funded research and development centers (FFRDC) on behalf of federal government sponsors. Identifying optimal alternatives for the critical functions of PIRAC Owner and Operator will provide the government with key information to facilitate implementation of the PIRAC concept to improve Payment Integrity.

1.2 Origin and Approach

Defending against fraud and other improper payments is a significant cross-government challenge. In fiscal year (FY) 2016, federal agencies estimated that they made more than \$144 billion in improper payments, representing the equivalent of the fifth largest federal agency. The amount of reported improper payments has more than tripled over the last decade, and these estimates do not include all agencies or programs.

In Congressional testimony in March 2015, David Mader, former United States Controller, Office of Management and Budget (OMB), stated that “the current levels of improper payment errors are unaffordable and unacceptable.”³ In addition to their significant economic impact on our nation, improper payments compromise public trust in government.

MITRE recognizes the impact that the overall federal Payment Integrity situation has on government effectiveness and public confidence. Given the public interest nature of this challenge, in 2015 MITRE conducted an independent study to assess the underlying systemic factors that enable fraud and other improper payments and to explore innovative government-wide solutions to improve Payment Integrity. Two key, related strategic recommendations in that study were (1) to explore PPPs to cost-effectively bring to bear needed information technology resources, data sets and skillsets otherwise unavailable; and (2) to establish a PIRAC—a shared, cross-government research and data analytics capability to be used to improve the prevention and detection of fraud and other improper payments.

¹ Payment Integrity refers to improper payments and the people, processes, and technology that are meant to ensure that the payments are actually proper.

² GOVERNMENT-WIDE PAYMENT INTEGRITY: NEW APPROACHES AND SOLUTIONS NEEDED ([MTR160040](#), February 2016)

³ Testimony of David Mader, United States Controller, OMB, before the Senate Committee on Homeland Security and Governmental Affairs, March 16, 2015

2 Overview of Public-Private Partnerships and the Payment Integrity Research and Analysis Capability Concept

Public-Private Partnerships involve long-term chartered collaboration among two or more government, commercial, or non-profit entities that results in mutual benefit. Historically, most PPPs have been for public works—providing a public good while placing the management and major share of risk on the private partner(s). In recent years there has been an increase in information-centric PPPs that serve as a focal point for the exchange of actionable insights, information and data among partners to address national issues in areas such as healthcare, homeland security, and transportation. Key elements of these information-centric PPPs often include rapid, robust communications and data fusion and analytics, which are facilitated by the PIRAC concept.

2.1 Public-Private Partnerships

Government services ecosystems are increasingly interconnected and involve multiple stakeholders with sometimes similar, and sometimes competing, interests. Further, agencies face emergent challenges such as economic realities and political complexities, coupled with obstacles to obtaining system-wide situational awareness. The ability of any one agency to accomplish meaningful change in these complex systems is limited by such factors as time, talent, technology, and the ability to influence or control the diverse set of stakeholders. Figure 2-1 notes selected challenges that may favor using a PPP to solve critical national problems.

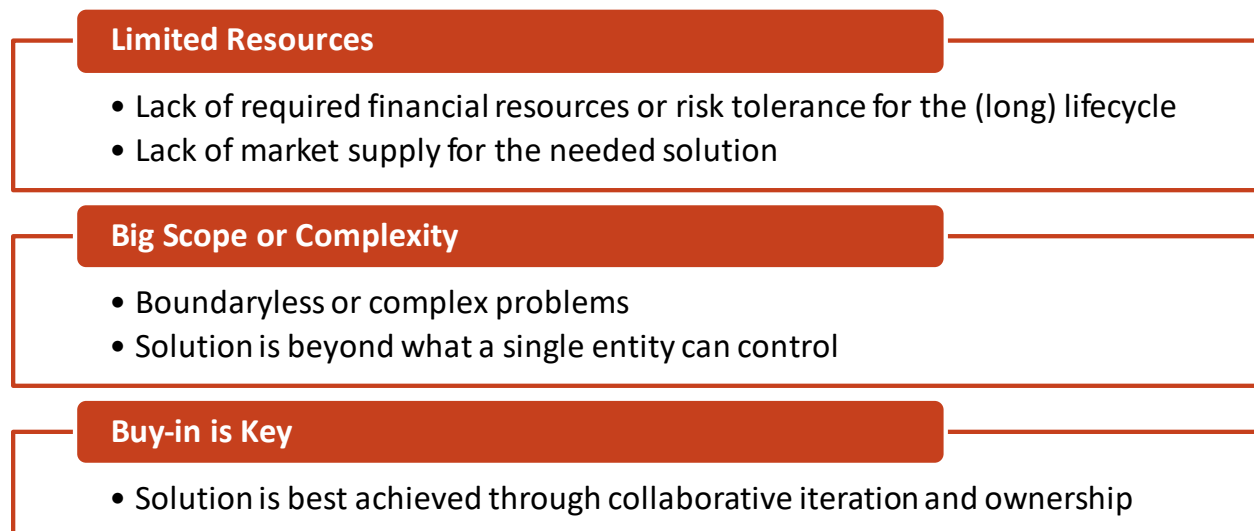


Figure 2-1. When to Consider a PPP

Source: MITRE Analysis

PPPs offer a potential solution by providing a way for government, commercial, academic, and non-profit entities to collaborate on issues of mutual interest and to realize benefits

that no single entity could feasibly achieve alone. Critical success factors of PPPs include the following.

- Accomplishing a common mission and purpose by:
 - Clarifying mutual and public benefit
 - Chartering the PPP to align interests and expectations
- Delivering value to the partners by:
 - Sharing the burden of time, labor, and investment
 - Connecting talent, technology, and techniques
 - Employing the most effective governance and business models, technologies, and protocols
- Building trust among partners by:
 - Delivering as expected
 - Communicating proactively and constantly
 - Ensuring accountability

The resulting PPP capability enables significant impact at relatively low cost to any given member of the partnership. There are many examples of agencies engaging in PPPs under established authorities.⁴ Two ongoing examples of successful Payment Integrity-related PPPs are the Healthcare Fraud Prevention Partnership (HFPP) and the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (IDTTRF-ISAC).

- The HFPP, sponsored by the Centers for Medicare and Medicaid Services (CMS), creates a collaborative advantage to combat healthcare fraud by joining nearly 80 claims paying organizations, associations, government and law enforcement agencies in a PPP. A key feature of the HFPP is harnessing the power of extensive data fusion and analytics. The HFPP:
 - Developed a broad, deep data pool and regular cadence of analytic studies that promote system-wide detection and prevention of fraud
 - Analyzes data sets for potential fraud—e.g., suspicious claims patterns in the data
 - Provides real time, secure peer-to-peer sharing of information about suspicious providers, fraud scheme blueprints, and misused payment codes
 - Has helped identify exposure, reduce losses, increase recoveries, and deter future fraud schemes, with \$260 million saved and 17,000 suspect providers identified
- The IDTTRF-ISAC, sponsored by the Internal Revenue Service, aims to reduce tax refund fraud by monitoring returns filed for patterns that might indicate potential fraud using stolen taxpayers' identities. Its partners include numerous states, the tax

⁴ The legal and policy support for PPPs is broad and well-established. Agencies can draw on existing authorities to collaborate and form partnerships under the Economy Act, Bayh-Dole Act, Federal Technology Transfer Act, and OMB guidance, as well as multiple agencies' policies and precedents. Agencies can fund or support PPPs via contracts, grants, Cooperative Research and Development Agreements, and Other Transaction Authority agreements.

industry, financial institutions, and tax return preparers. The IDTTRF-ISAC PPP is being piloted during the 2017 and 2018 tax filing seasons.

Other Payment Integrity challenges suggest the potential for PPPs to add value to the government's fight against improper payments. For example, in the area of disability payments, multiple federal agencies, state agencies, and insurance organizations make healthcare and benefits payments to individuals. Similarly, multiple federal agencies, state and local governments, and insurance organizations are involved in paying benefits during the response to and recovery from natural disasters. In both of these examples (as well as the HFPP and IDTTRF-ISAC above):

- Large numbers of individuals and many billions of dollars of payments are involved
- There is a history of fraud
- Multiple data sets exist that would benefit from coordinated sharing and analytics
- Numerous stakeholders would benefit from information sharing on leads, techniques, etc.

With regard to Payment Integrity, PPPs focused on cross-government issues and challenges have proven to be a cost-effective means of helping to identify and prevent errors and deter fraud. Key elements of this approach include the critical success factors above, manifested in information sharing, data sharing and analytics, and the involvement of a conflict-free trusted third party—all of which are also integral to the PIRAC concept. The PIRAC concept is, in essence, the operational component of Payment Integrity PPPs.

2.2 The PIRAC Concept

2.2.1 Mission

The mission of a PIRAC is to enhance the prevention and detection of fraud and other improper payments.

2.2.2 Vision

The vision of a PIRAC is to be a leader in advanced data analytics to improve Payment Integrity across the government. A PIRAC will serve as a collaborative hub to not only enable agencies to better identify potentially improper payments during processing, but also, and even more importantly, to enhance agencies' ability to use a *left of check* approach—a shift in focus from catching errors during processing and expensive, flawed *pay & chase* methodologies, towards applicant error prevention and fraud deterrence. See Figure 2-2.

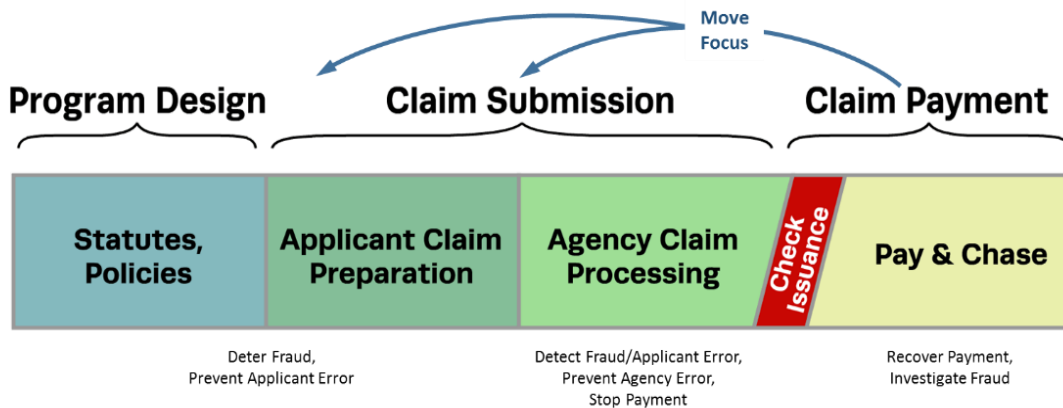


Figure 2-2. Illustration of *Left of Check* Concept

Source: MITRE Analysis

In combating improper payments, agencies usually adopt defensive strategies around catching errors during processing as opposed to preventing applicant errors/detering applicant fraud. Even worse, agencies often make payments and then attempt to identify and recover those that are improper. However, it is generally less expensive and risky to prevent applicant errors and deter applicant fraud. This is *left of check* thinking, i.e., the further to the left of (before) the issuance of a payment in the overall process that the payment is stopped, the less expensive and risky to the organization. The worst case is to make improper payments and then attempt to recover them—called *pay & chase*—which Government Accountability Office officials have labeled as fundamentally flawed.

2.2.3 Key Operational Concepts

Some experts maintain that without automation, organizations will never be able to catch up with the ever-changing tactics of fraudsters. As such, analytics represent an accelerator of capabilities, allowing organizations to score, predict, correlate, and uncover emerging behaviors much faster than any other way.

As shown in Figure 2-3, a PIRAC will centralize data (open source, commercial, and as appropriate, government), use advanced analytical tool sets (open source, commercial, and, as appropriate, government-developed), and dedicate a team of internal and external specialists to error and fraud prevention and detection activities. It will use a federated approach which will include collecting multiple data sets and testing/measuring the value of analytic approaches that cannot be conducted today without the use of these multiple data sets across multiple tools. The concept emphasizes communications—sharing best practices, collaborating on solving systemic improper payments problems, and developing information exchange mechanisms similar to the near-real-time efforts of ISACs.



Figure 2-3. High-Level Overview of a PIRAC

Source: MITRE Analysis

A number of data analytics efforts are currently in place or being adopted by government agencies. Examples of those efforts include:

- The Treasury Department’s Do Not Pay (DNP) solution and the Bureau of the Fiscal Service’s Philadelphia Financial Center, assisting agencies with pre-pay and post-pay analytics, respectively
- CMS’ Fraud Prevention System, a predictive analytics technology used to identify and prevent fraud in the Medicare program
- The Department of Labor’s Unemployment Insurance Integrity Center of Excellence, a federal-state partnership that facilitates the development and implementation of integrity tools by the states and shares best practices in the detection and reduction of improper payments
- The General Services Administration (GSA), which is developing a collection of data analytics tools to assist agencies in monitoring and preventing improper payments in government charge card programs

A PIRAC will complement and augment those data analytics efforts—not replace them. And while those efforts are targeted, in many cases siloed, solutions, a PIRAC will, instead, provide a systemic solution for use across multi-agency domains and with government-wide issues, as well as by individual agencies and programs.

The PIRAC vision aligns with key mandates of the bi-partisan Fraud Reduction and Data Analytics Act of 2015 (P.L. 114-186). The Act requires that federal agencies establish financial and administrative controls in order to identify and assess fraud risks, and design and implement control activities in order to prevent, detect, and respond to fraud and other improper payments. The Act further requires agencies to collect and analyze data from reporting mechanisms on detected fraud to monitor fraud trends, and to use that data to continuously improve fraud prevention controls. Finally, the Act mandates the

development of a plan for establishing and using a federal interagency library of data analytics and data sets, which can incorporate or improve upon existing federal resources and capacities, for use by agencies and Offices of Inspector General to facilitate the prevention and detection of fraud and other improper payments. Success will require the best in advanced data analytics together with complete and current data; expertise in fraud schemes, strategies, pathways, and vulnerabilities; and collaboration between all stakeholders. These success criteria are the basic components of a PIRAC.

3 Methodology for Assessing PIRAC Owner and Operator Alternatives

A methodology used for Assessment of Alternatives that involves the a priori definition of the alternatives and evaluation (scoring) based on insights from research and evidence gathering may be used for assessing PIRAC Owner and Operator alternatives.

3.1 Background Research

To gather insights and lessons learned from similar information exchange and data analytics efforts, we reached out across MITRE and surveyed relevant literature. We included in that MITRE outreach information gathering and interviews with representatives of the following large-scale successful MITRE analytics environments and labs: the Aviation Safety Information and Sharing program, the IDTTRF-ISAC, the HFPP, the Holistic Analytics Environment, the Analysis Tool Shed Lab, the Enterprise Technology Lab, and the Symphony Enterprise Strategic Initiative development team. We obtained leading practices and considerations for analytic partnerships from this research and outreach, which were then used to inform the methodology.

3.2 PIRAC Owner and Operator Definitions

To assess the totality of PIRAC operations, four roles were identified as follows. See also Figure 3-1.

- **Owner**—The Owner charters and controls a PIRAC and provides necessary resources such as funding and staff. The Owner may draw on expertise from an entity fulfilling the Facilitator role (below) to define and instantiate a PIRAC. The Owner is accountable for a viable and functional PIRAC.
- **Operator**—The Operator is the primary user-facing entity that creates a PIRAC environment and manages the day-to-day PIRAC operations including logistics, projects, membership, activities, and communications. They also operate the supporting technologies, production-level services, and capabilities for a PIRAC—particularly those that are user-facing such as a collaboration portal and service desk tools. The environment created will meet user expectations for security, privacy, and independence and have the ability to import data from stakeholders and export it to the portal. They may own, outsource, or interact with a separate entity that fulfills the Analytics Provider role (below). The Operator may determine what capabilities are best to perform internally vs. outsource.
- **Facilitator**—The Facilitator defines, frames, and advises on PIRAC structure and capabilities, conducts prototypes, and evaluates and acquires (but does not operate) solutions and solution providers. This role is similar to the expert advisory and acquisition support role that FFRDCs often perform for government sponsors.
- **Analytics Provider**—The Analytics Provider delivers the core PIRAC solution (i.e., analytics expertise [staff], tools, datasets, and protocols) to perform secure data analytics at scale. This solution would be tailored to a customer’s needs across a full range of support options (e.g., full service, do-it-yourself). The Analytics Provider

will expect the information technology environment to provide needed flexibility and scalability on demand, and may determine what capabilities are best to perform internally vs. outsource.

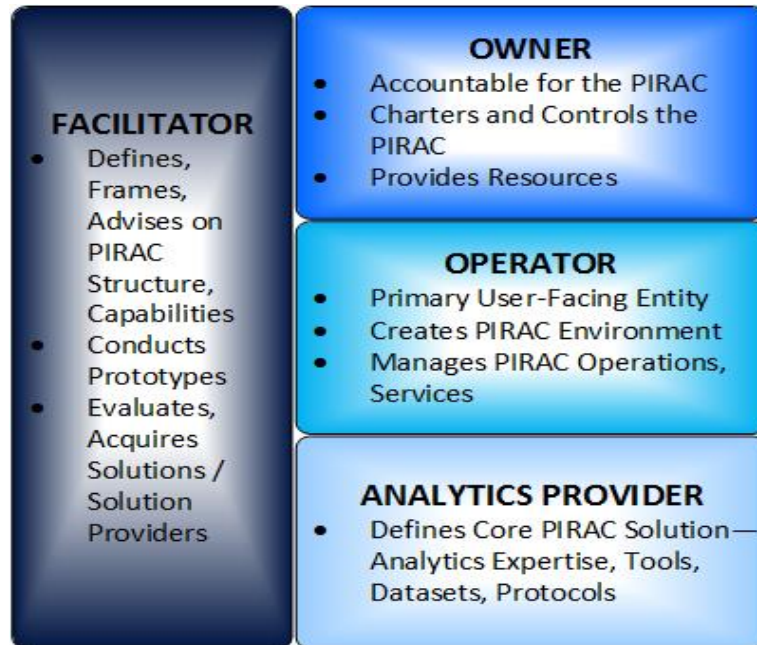


Figure 3-1. PIRAC Roles

Source: MITRE Analysis

The same entity may perform all four roles, or different entities may perform each role or combinations of roles. For this report, we focused on the Owner and Operator roles.

3.3 Alternatives Considered

Based on insights gleaned from the evidence-gathering approach described in Section 3.1, we identified four types of entities that could serve in the Owner or Operator roles:

1. Government Agency (a single agency, e.g., OMB, Treasury, GSA)
2. Government Group (e.g., a working/leadership group)
3. For-Profit Entity (e.g., commercial service provider/integrator)
4. Not-for-Profit Entity (e.g., a foundation, academic institution, FFRDC, or non-profit Limited Liability Corporation [LLC])

While other formulations are possible, we found that these four fairly represent the breadth of legal entity types commonly found in analytic partnerships.

3.4 Evaluation Criteria

Based on the analysis and research described in Section 3.1, we identified 14 evaluation criteria that are relevant to an entity that would fulfill the PIRAC Owner and/or PIRAC Operator roles, as shown in Table 3-1.

Table 3-1. Evaluation Criteria

Criterion [The Owner or Operator is...]	Definition	Relevant to
1. Able to secure funding	Ability to obtain sufficient funding for start-up and operations	Owner
2. Able to use many funding sources	Ability to obtain/accept multiple funding streams	Owner
3. Able to readily establish the PIRAC	Ability to instantiate the PIRAC including legal considerations and stakeholder acceptance (e.g., level of participation, data sharing)	Owner
4. Accepting of mission/risk	Level of risk tolerance to accomplish mission	Both
5. Able to convene stakeholders	Ability to bring together a diverse set of stakeholders under a manageable organization construct (recognizing any legal restrictions or partner equities)	Both
6. Able to collaboratively govern	Ability to support equitable, inclusive decision making and fairly align partner interests with common goals	Both
7. Trusted with government data	Ability to handle law enforcement, identity and eligibility verification, and other sensitive/identifying data	Operator
8. Trusted with partner data	Ability to handle non-government partners' proprietary and sensitive data given privacy, security, and legal considerations	Operator
9. Able to obtain data	Ability to negotiate Data Use Agreements and navigate approvals	Operator
10. Able to be responsive	Ability to meet stakeholder expectations for timeliness and solution provided	Operator
11. Proven in advanced data analytics	Demonstrated successful performance/track record of advanced data analytics	Operator
12. Proven in research studies	Demonstrated successful performance of research studies	Operator
13. Proven in information exchange	Demonstrated successful performance of facilitating regular information (e.g., fraud schemes and perpetrators) exchange among partners	Operator
14. Proven in domain expertise	Demonstrated experience in related areas (e.g., fraud, other improper payments, agency operations and challenges)	Operator

As noted in the definitions in Section 3.2 above, the Owner has responsibility for a viable and functional PIRAC. As such, criteria 1–6 addressing viability of funding, legal agreements, risk acceptance, and effective governance are relevant to the Owner. Because the Operator is integral to the ongoing delivery of PIRAC services and is the “face” of a PIRAC to the stakeholders and partners, they also must be willing to accept the mission risk

and foster effective governance while addressing partners' expectations for responsiveness, data handling, and relevant expertise. However, the Operator does not have direct responsibility for funding and establishing a PIRAC. As such, criteria 4–14 are relevant to the Operator.

3.5 Rating Scale and Weighting

The rating scale for each criterion is based on a qualitative assessment scale with three points: High, Medium, and Low. Research showed that central to the success of a PIRAC were the ability to be trusted with data, meet stakeholder expectations, and manage diverse stakeholders. To that end, we determined that five criteria were especially important to the success of a PIRAC:

5. Able to convene stakeholders—Creating a constructive and safe working environment for stakeholders to meet physically and virtually. Drawing on established relationships and building new ones to bring partners to the table. Encouraging open discussion of complex and potentially challenging topics. Fostering progress toward mutual goals through effective outreach, communications, facilitation, and event management.
6. Able to collaboratively govern—Creating a shared sense of ownership and allowing partners' voices to be heard and acted upon. Supporting mutually agreeable decision-making protocol and expectations. Promulgating a culture of mutual respect in the context of recognizing partners' equities and accountability to each other in shaping the governance of the partnership.
7. Trusted with government data—Delivering expected security and privacy safeguards while maintaining independence regarding data oversight by any one party, as appropriate. Fostering shared interest in the appropriate and protected use of partners' data to achieve desired outcomes. Providing assurances that sensitive data can be properly handled through consistently aligned actions.
8. Trusted with partner data—Methods presented in “Trusted with government data,” plus assuring commercial entities that concerns regarding intellectual property use, competitive advantage, Freedom of Information Act requests / discoverability, and potential blowback (e.g., regulatory or investigative consequences of sharing with the partnership) are addressed.
10. Able to be responsive—Meeting industry expectations for timeliness, value, and level or quality of service. Clearly and consistently communicating and managing expectations. Providing customer-centric service and product delivery.

Given the importance of these criteria in assessing alternatives, the scores for these five criteria should be weighted more heavily (e.g., twice that of the other criteria).

The assigned High, Medium, and Low qualitative assessments for each entity/criterion combination should be converted to quantitative scores of 5, 3, and 1 respectively (based on modified Fibonacci sequence). These raw scores then need to be multiplied by the weighting factors to arrive at a total entity/criterion score for the Owner (Table 3-2) and the Operator (Table 3-3) below.

The six criteria of importance to the Owner role should be scored as shown in Table 3-2.

Table 3-2. Scoring PIRAC Owner

Criterion (Weight) [The Owner/Operator is...]	Govern- ment Agency	Govern- ment Group	For- Profit Entity	Not-for- Profit Entity
1. Able to secure funding (1x)				
2. Able to use many funding sources (1x)				
3. Able to easily establish PIRAC (1x)				
4. Accepting of mission/risk (1x)				
5. Able to convene stakeholders (2x)				
6. Able to collaboratively govern (2x)				
<i>Weighted Score</i>				

The eleven criteria of importance to the Operator role should be scored as shown in Table 3-3.

Table 3-3. Scoring PIRAC Operator

Criterion (Weight) [The Owner/Operator is...]	Govern- ment Agency	Govern- ment Group	For- Profit Entity	Not-for- Profit Entity
4. Accepting of mission/risk (1x)				
5. Able to convene stakeholders (2x)				
6. Able to collaboratively govern (2x)				
7. Trusted with government data (2x)				
8. Trusted with partner data (2x)				
9. Able to obtain data (1x)				
10. Able to be responsive (2x)				
11. Proven in advanced data analytics (1x)				
12. Proven in research studies (1x)				
13. Proven in information exchange (1x)				
14. Proven in domain expertise (1x)				
<i>Weighted Score</i>				

Based on the results of scoring a specific scenario, the optimal type of entity to fulfill an Owner or Operator role will be apparent.

4 Key Takeaways

While we identified 14 criteria that are relevant to any entity that would fulfill the PIRAC Owner and/or PIRAC Operator role, the most critical factors to consider in analyzing Owner and Operator alternatives are the ability to:

- Convene stakeholders
- Collaboratively govern
- Be trusted with government data
- Be trusted with partner data
- Be responsive

While a PPP needs a PIRAC if it will be engaged in analytics and/or information sharing, there is no single PIRAC Owner and Operator model that necessarily works for every PPP. Consequently, members of a PPP need to do their own assessment of PIRAC Owner and Operator alternatives for that specific PPP, using the methodology in Section 3.

As noted above, the chartering of a PPP should be purpose-suited to the partners' shared mission and aligned with their interests and abilities. Our experience has been that the optimal Owner may be that entity with the greatest authority and/or initial funding for a given mission, provided they can effectively form and guide the PPP *in partnership*. Related, our research has also shown that the Operator (sometimes referred to as a trusted third party) is most successful when they provide the appropriate level of independence (i.e., are able to resist any one partner's undue influence) and embody freedom from conflicts of interest, especially when handling partners' sensitive data.