

**The critical connection between established security and protection practices and business practices *is the new emphasis* in the field of Risk Management of Outsourced Network Services**

# USER MANUAL: THE OUTSOURCING NETWORK SERVICES ASSESSMENT TOOL (ONSAT)

**For use with ONSAT Basic Version 5.0 dated 6/23/2020**

## **Abstract**

This document serves as a user manual for the Outsourcing Network Services Assessment Tool (ONSAT). ONSAT is a tool that provides public and private organizations of all sizes, a comparative understanding of the risks associated with outsourcing network services to second and third party vendors. ONSAT supports a broad audience of government, large industry, as well as small and medium businesses. This associated user manual is a systematic guide to assist whomever in the organization would normally complete risk assessments / respond to risk management requests. ONSAT implements a consistent analytic approach using related assessments to assess if, and how well, potential outsourcing partners and their suppliers implement security and business practices. ONSAT's Business Assessment includes questions about the business investments of companies providing outsourced network services derived from The Committee on Foreign Investment in the United States' (CFIUS) Joint Voluntary Notice. ONSAT's Security Assessment aligns to ten established frameworks and standards with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) as the overarching standard. ONSAT's Financial Assessment assigns each decision alternative a cost utility value based on the service cost for each provider, the role of the provider in the decision alternative, and a user-defined maximum budget. ONSAT leverages available evidence and subject matter expertise to inform individual and aggregated displays as well as, analysis of decision alternatives to "rack and stack" recommended courses of action to inform risk management decisions.

## Table of Contents

Acknowledgements.....	4
Note to the Reader: .....	4
1.0 Introduction .....	7
1.1. Risk Management of Decision to Outsource Network Services .....	7
1.2. “Trust Relationships” Associated with Outsourcing .....	8
1.3. Understanding the Security and Trust Boundary .....	9
1.4. ONSAT as a Decision Aid .....	10
1.5. The Component of Risk Addressed by ONSAT .....	12
2.0 Inside ONSAT.....	13
2.1 Overview of ONSAT Architecture and Components .....	13
2.1.1 Business and Security Frameworks.....	14
2.1.1.1 Business Investment Framework.....	14
2.1.1.2 Security Frameworks and Standards .....	14
2.1.2 Business Trust and Security Maturity Categories .....	15
2.1.2.1 Business Trust Categories .....	15
2.1.2.2 Security Maturity Categories .....	16
2.1.3 Business Trust and Security Maturity Assessments and Associated Scales.....	17
2.1.3.1 Business Trust Assessment Questions .....	17
2.1.3.2 Business Assessment: Information Verification Scale .....	18
2.1.3.3 Business Trust Assessment: Information Trust Basis Scale .....	19
2.1.3.4 Security Maturity Assessment Questions .....	19
2.1.3.5 Security Assessment: Security Maturity Scale .....	20
2.1.4 Financial Assessment and Associated Scale.....	21
2.1.5 Display of Results and Integrated Decision Alternatives .....	22
2.1.5.1 Individual Provider Results and Summary Views.....	22
2.1.5.2 Aggregated Results and Integrated Decision Alternative Displays.....	22
2.1.6 Overview of ONSAT Tabs .....	23
3.0 Using ONSAT to Conduct an Assessment.....	24
3.1 Step 1: Define Outsourcing Problem and Decision Alternatives .....	25
3.1.1 Step 1a: Defining the Outsourced Network Service(s) Characteristics.....	26
3.1.2 Step 1b: Defining the Outsourced Network Service(s) Requirements .....	27
3.1.3 Step 1c: Defining the Potential Providers to be Assessed .....	28

3.1.4	Step 1d: Defining the Decision Alternatives (Combinations of Providers)	31
3.2	Step 2: Collect and Appraise Evidence	34
3.2.1	Defining Evidence	34
3.2.2	Sources and Examples of Evidence	35
3.2.3	Appraising Evidence	36
3.3	Step 3: Accept Default Tool Settings	36
4.0	Step 4: Assess Providers Using Evidence	37
4.1	Identify the Individual or Team Conducting the Assessment	37
4.2	Define the Internal Process	38
4.3	Conduct a Business Trust Assessment	39
4.4	Conduct a Security Assessment	41
4.5	Conduct a Financial Assessment	43
5.0	Step 5: Examine Assessment Results and Analyze Decision Alternatives	48
5.1	Individual Provider Results	49
5.1.1	Business Trust	49
5.1.1.1	Provider Business Display	49
5.1.1.2	Provider Business Category Display	50
5.1.2	Security Maturity	51
5.1.2.1	Provider Security Display	51
5.1.2.2	Provider Security Category Display	52
5.2	Summary Views	54
5.2.1	Business Summary	54
5.2.2	Security Summary	55
5.2.3	Financial Summary	57
5.3	Aggregated Results and Integrated Decision Alternative Displays	58
5.3.1	Provider Integrated Display	58
5.3.2	Decision Alternative Business Display	59
5.3.3	Decision Alternative Security Display	61
5.3.4	Decision Alternative Financial Display	63
5.3.5	Decision Alternative Score Summary	65
5.3.6	Decision Alternative Integrated Display	68
5.3.7	Total Value Display (Ranked)	69
5.3.8	Total Value Composite Chart	71

5.4	Final Decision Support Analysis .....	72
5.4.1	Overview of Deeper Analysis of the Top Decision Alternatives.....	72
5.4.2	General Observations: Decision Alternatives Compared to Current Operations.....	73
5.4.3	Additional Findings: Top Decision Alternatives Compared to Current Operations .....	75
5.4.4	Financial Cost Savings: Top Decision Alternatives Compared to Current Operations.....	77
5.4.5	Business Trust Analysis: Top Decision Alternatives Compared to Current Operations.....	78
5.4.6	Security Maturity Analysis: Top Decision Alternatives Compared to Current Operations.....	79
5.4.7	Changing Decision Criteria Weights.....	81
6.0	Step 6: Present Findings and Provide Recommendations .....	83
6.1	Preparing the Presentation to Decision Makers.....	83
6.2	Summary of Findings.....	84
6.2.1	Findings about Current Internally Provided Network Services.....	84
6.2.2	Findings about Outsourcing Alternatives.....	85
6.2.2.1	Comparison of Decision Alternatives Overall Assessment Scores .....	85
6.2.2.2	Comparison of Remaining Decision Alternatives Scores .....	85
6.2.2.3	Comparison of the Remaining Alternatives Scores by Criteria Contributions.....	86
6.2.2.3.1	Comparison of Remaining Decision Alternatives: Financial Cost.....	87
6.2.2.3.2	Comparison of Remaining Decision Alternatives: Business Trust and Security Maturity...	87
6.2.3	Comparison of Two Best Options with Redefined Weights.....	88
6.3	Review of Self-Assessment to Inform Business Goals .....	89
6.3.1	Review of Self-Assessment: Business Trust .....	89
6.3.2	Review of Self-Assessment: Security Maturity .....	90
6.3.3	Business Goals Informed by Self-Assessment.....	91
6.4	Decision Recommendations: Option 1 and Option 2 .....	92
7.0	References for Additional Reading .....	93
8.0	Glossary: Lexicon & Terminology.....	93
	Annex 1: Mapping of Security Frameworks and Guidance to Categories .....	98
	Annex 2: Business Assessment .....	101
	Annex 3: Security Assessment .....	103
	Annex 4: Tool Settings Adjustment.....	108



## Acknowledgements

The Outsourcing of Network Services Assessment Tool (ONSAT) and this User Manual are the culmination of an effort by a group of dedicated professionals from across Government and Private Industry. ONSAT is a decision aid that brings risk-based information into the decision-making process so that the benefits, financial costs, security risk cost, and business risk cost collectively inform critical outsourcing decisions.

ONSAT is available as a public service without copyright or restrictions on use.

ONSAT and its availability to the public would not have been possible without the significant contributions of Willard Unkenholz, the tool developer, and Christine E. Thompson, Project Manager and user manual lead, both from the National Security Agency, as well as, significant user manual contributions by Lisa Meenen from Noblis, Inc. Substantial Contributions by Craig Herrick of DISA enabled pilot review and promoted feedback for tool functionality.

Significant Private Industry contributions from Greg Blackwell, John Nagengast, Shane Steiger, Bruce Weed, and Stephen Whitlock underpinned tool design and functionality, enabled critical testing and review, and informed user manual content.

## Note to the Reader:

This document is a user manual not a quick start guide. Although a user manual and quick start guide both focus on getting the user “up and running” with software, a product, or a service as soon as possible, a user manual is expected to provide more in-depth information and instruction than a guide. With this distinction made, below is some information to assist your navigation and application of the user manual.

### **Audience:**

- The manual is written as a decision aid supporting:
  - Businesses or organizations considering outsourcing network services, the business functions that support network features, components, and applications i.e. (e.g. web/internet services, cloud computing, teleconferencing, etc.). A broader listing of the common types of network services are included in the *Network Services and Tool* Tab.
  - Businesses or organizations vetting outsourcing decisions,
  - Users with a basic understanding of business contracts and outsourcing relationships (e.g. outsourcing organization, prime, sub, third party vendors)
  - Users with a basic understanding of network service outsourcing and network security issues including both technical implementation and business management.
  - Training related to Acquisition, Supply Chain Risk Management, Business Management, Financial Cost Utility, etc.
  - Experts from different communities who would like to use the tool to tailor scenarios, add analytics, or expand the tool’s functionality, etc.

### **Tool Format:**

- ONSAT is a prototype in an MS EXCEL spreadsheet format and is the basic version.
- Other implementation platforms, enhanced features, and better data and functional management can be achieved in other formats; however, Excel provides a level playing field for smaller businesses and organizations.

- More advanced tailoring of the tool as well as more advanced analysis techniques can augment this basic version.
- Tool issues may actually be MS EXCEL issues and a quick web search may answer the question.

### **Arrangement / Layout:**

The User Manual has eight sections and four annexes. A brief description is provided below.

- **Section 1: Introduction:** Purpose of ONSAT in the current network services and outsourcing environment.
- **Section 2: Inside ONSAT:** Structure and components of the tool including business and security frameworks, categories, questions and scoring scales that comprise the assessment.
  - Section 2.1.6 provides an overview of the tabs within the tool.<sup>1</sup>
  - *Flow of the manual aligns with the order of the tool tabs; beginning with the assessment tabs, the tab order is Business Trust, Security Maturity, and Financial Cost Utility.*
- **Section 3: Describes the 6 Steps to Complete an Assessment and Covers the first three steps.**
  - **Step 1:** Defining the Scenario and Decision Alternatives and Identifying the Providers to be Assessed
  - **Step 2:** *Perform Outside the Tool* – Gather evidence, assemble the team, and review Internal guidance
  - **Step 3:** Accept tool defaults
- **Section 4: Conducting the Assessment**
  - **Step 4:** Step by Step instructions to conduct an assessment.<sup>2</sup>
    - *Flow of this section is a high level description, details of each task, and guidance on completion to the user.*
- **Section 5: Examining the Results using ONSAT Displays**
  - **Step 5: Examining Provider and Aggregated Displays and Analyzing Alternatives**
    - Display Sections: Provider, Summary, and Decision Alternatives
      - *Flow of this section is a high level description, key information provided by the display, and additional analysis or tasks prompted by the display.*<sup>3</sup>
    - Final Decision Support Analysis and Changing Criteria Weights are also covered.
- **Section 6: Decision Recommendations**
  - **Step 6:** *Perform Outside the Tool* – Present Findings and Provide Recommendations
  - *Flow of this section is Finding, then briefing slide with key points and visual representations; the last briefing slide presents recommendations.*
- **Section 7: References for Additional Reading**
  - Key references are listed including-*An Approach to Assessing Vendors to Lower Potential Risk of Outsourced Network Services, The Open Group Guide*, a related resource tapping some of the same subject matter experts that that discusses the topic of Outsourcing Network Services in detail, cites ONSAT as a decision aid, and provides best practices and recommendations from pre-contract through recovery phases.
- **Section 8: Glossary: Lexicon and Terminology (also see Tool Terms).**

---

<sup>1</sup> ONSAT Basic Version contains a set of completed (prepopulated) tabs using the cloud data storage scenario detailed in the *Outsourced Service Definition* Tab.

<sup>2</sup> The cloud storage data scenario with example providers and assessment data is used throughout the manual.

<sup>3</sup> **Note 1: A Closer Look** –a breakout box focusing on an area that the subject matter experts from the working group highlighted based on current trends and best practices in the business and technical environments.

- In this user manual, terms are first and foremost defined for practical use of the tool and secondly by known industry standards as applicable to supply chain risk management.
- **Annex 1: Mapping of Security Frameworks and Guidance to Categories**
  - Categories in ONSAT's Security Assessment are mapped to critical controls and guidance derived from individual security frameworks. The mapping enables users to apply ONSAT knowing that there is linkage to recognized security guidance and frameworks. A complete mapping of security categories and frameworks is included in the *Security Frameworks Mapping* Tab in the tool.
- **Annex 2: Business Assessment**
  - A complete copy of the Business Trust Assessment.
- **Annex 3: Security Assessment**
  - A complete copy of the Security Maturity Assessment.
- **Annex 4: Tool Settings Adjustment**
  - The "Tool Adjustment Settings" section of the tool contains individual tabs available to input *user-defined values* that modify the content and/or weight of criteria.

**Miscellaneous:**

- **Links / Websites:** current as of date of publication or retrieval date cited or if no date cited, current as of the date of the User Manual.
- **Graphics:**
  - Entire visual representation of content may not be displayed due to space limitations, usually noted as follows: "*Due to space limitations, the entire worksheet may not be displayed or certain fields / columns may be abbreviated.*"
  - Graphics are a combination of text and color to ensure usability by all.
- **Tool Terms:** Every effort has been made to use tool terms consistently in the User Manual based on the naming conventions in the Tool. However, there are known variations, often due to space limitations in the tool or in the graphic program.
  - **Proper Name Examples:**
    - Overall = Aggregated = Aggregated Total
      - e.g. Overall Assessment Score = Aggregated Total Score = Aggregated Decision Alternative Score
      - Overall Business Trust Score = Aggregated Total Business Trust Score
    - Business = Business Trust
    - Security = Security Maturity
    - Financial = Financial Cost\*
      - \*Financial Cost Score and Financial Cost Utility Value / Score refer to the "Utility Value of the Cost" Score that enables score comparisons with scores for Business Trust and Security Maturity.
      - \*Financial Cost or Financial Cost Savings are monetary descriptors (\$).
  - **Other Examples:**
    - Provider = partner = supplier
    - outsourcing organization = *Self Now* = current operations
    - prime = prime contractor
    - sub = sub contractor

## 1.0 Introduction

### 1.1. Risk Management of Decision to Outsource Network Services

The effective and efficient accomplishment of many, if not most, critical governmental and business functions are highly dependent upon network computing and the security that those networks provide in protecting the confidentiality, integrity, and availability of critical, essential, and sensitive information and network service functions. At the same time, the cost and the amount of resources needed to provide and secure these functions and associated information has also increased. In today's age of open sourcing and flexible infrastructure, the concept of outsourcing a company's Information and Communications Technology (ICT) environments is therefore very attractive based on costs, resource allocation, and shifting risk to others.

To most efficiently and effectively provide and protect critical functions and information, public and private organizations are more and more looking at the economic and security benefits and costs associated with outsourcing all or portions of their critical network services. The decision to outsource critical network services, and to whom to outsource, is therefore a major risk management decision that can have corporate implications well beyond the parochial issues of Information Technology (IT) consequences. It can affect how well an organization can execute its primary business activities, protect sensitive, proprietary, corporate and client information, and secure its future reputation for being a trustworthy business partner or service provider.<sup>4</sup>

To make these risk management decisions, decision-makers need an understanding of the relative costs and risks associated with alternative decision options. There are often existing assessment practices and routines for determining the capability of potential network service outsourcing alternatives and in evaluating the economic viability of various business arrangements. There are often fewer existing processes for effectively highlighting the corporate and downstream client risks associated with these same network service-outsourcing alternatives to help inform those risk management decisions. For a more thorough discussion on risks associated with outsourcing network services, and guidance on proactively building and strengthening an organization's optimal set of business and technical practices leverages best practices and recommended frameworks and standards, refer to *The Open Group Guide: An Approach to Assessing Vendors to Lower Potential Risk of Outsourced Network Service*<sup>5</sup>.

Overall, the risks associated with outsourcing network services are not new nor are they unique to outsourced network services. However, these same issues are potentially exacerbated when, through contractual outsourcing relationships, we entrust the security of our mission and business critical information, systems, functions, and infrastructure to second and third parties providing outsourced network services. Organizations tend to make outsourcing decisions based primarily on whether or not an IT service can be performed more cost-effectively (from a performance stand-point) inside or outside an organization causing costs associated with risk to not be adequately considered. The Outsourcing of Network Services Assessment Tool (ONSAT) addresses this gap.

---

<sup>4</sup> **Note 2:** For this user manual, terms are first defined for practical use of the tool and secondly by known industry standards as applicable to supply chain risk management. The terms "organization," "partner," and "provider" are interchangeable with use based on the role in the outsourcing process.

<sup>5</sup> [www.opengroup.org/library/g197](http://www.opengroup.org/library/g197)

## 1.2. “Trust Relationships” Associated with Outsourcing

Any time the security of a critical business element is dependent upon a “trust” relationship, it is worth considering whether the potential mission, business, and financial gains associated with outsourcing are commensurate with or exceed the potential immediate and long-term consequences if the “trust” relationship is violated. A sufficient understanding of the “trustworthiness” of potential partners and their suppliers, along with sufficient insight, oversight, and enforceable accountability is necessary in order to effectively and safely manage that trust relationship.

Thus, in any outsourced service relationship, there is a defined and assumed trust relationship established with those performing the outsourced services. Organizations should strive for, *at a minimum*, the same level of trust afforded the in-house component and/or account for the risk when it is disparate. Furthermore, the outsource partner is expected to perform the outsourced services at a reasonable, manageable, and competitive resource cost, without putting the mission/business critical information and functions or the industry reputation of the outsourcing client or their customers at a significant risk.

Four potential main types of “trust” relationships exist as part of an outsourced network service. Each trust relationship carries security responsibilities that, in turn, corresponds to business “Care Abouts” for the outsourcing organization (Figure 1). For more information on trust models, please refer to “An Integrative Model of Organizational Trust”<sup>6</sup> and NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing.<sup>7</sup>

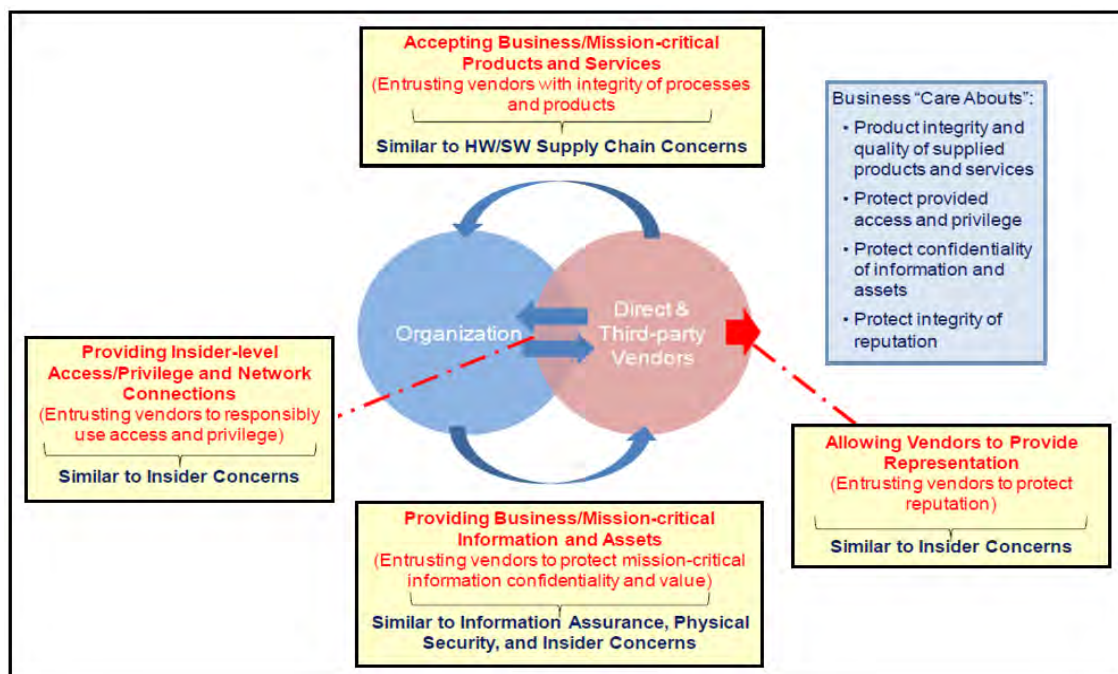


Figure 1: Outsourced Trust Relationships and Business “Care Abouts”

<sup>6</sup>An Integrative Model of Organizational Trust, July 1995, Academy of Management Review, 20(3), 709-734; Mayer, R.C., Davis, J.H., Schoorman, F.D.: retrieved from: <http://www.jstor.org/stable/258792>

<sup>7</sup> NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing; refer to: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

### 1.3. Understanding the Security and Trust Boundary

Understanding trust relationships and managing them is an important aspect of managing the risks of outsourcing network services. Through outsourcing, the security and trust boundary is essentially extended beyond the personnel, resources, systems, and facilities of the outsourcing organization, to include the personnel, resources, systems, and facilities of the outsource partners and their support partners (Figure 2).

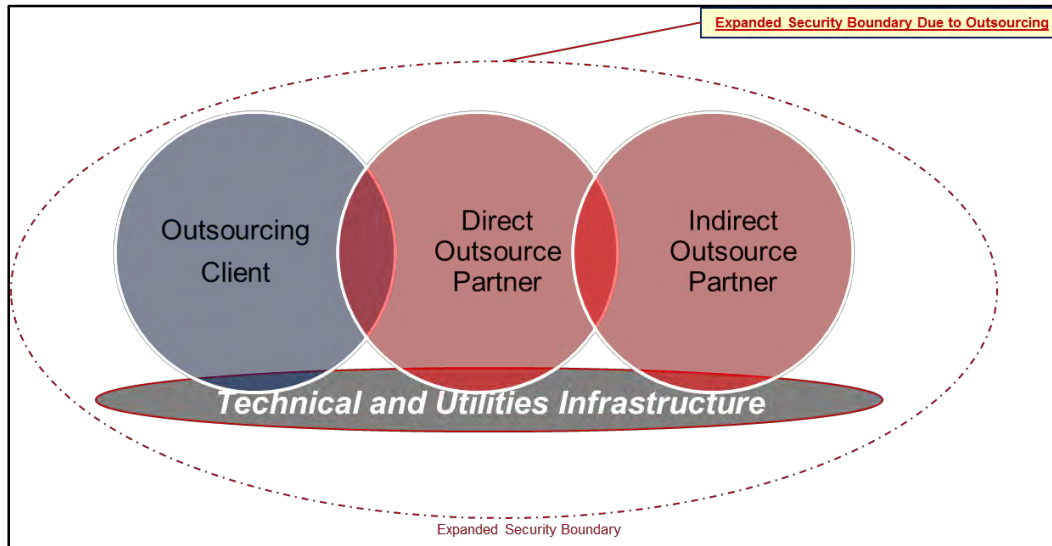


Figure 2: Extended Security Boundaries Due to Outsourcing

The extent of direct control an organization has in mitigating and controlling potential risks is much greater when performing network services in-house. An organization, using their established risk management processes and practices, can assign and prioritize resources based on their own evaluation of the potential risks to their critical information and functions and risk tolerance. Services performed by the outsourced partner(s)/vendor(s) become more difficult for the outsourcing organization to mitigate and control potential risks.

When extending the security boundary to outsourced partner(s)/vendor(s), equivalent or better protection and preservation of the confidentiality, integrity, and availability of mission/business critical information and functions must also be extended. This interdependency is depicted in Figure 3 on the next page. Successful Mission and/or business operations and the reputation of the business are dependent on defining and enforcing protection of critical information and systems functions that, in turn, are dependent upon implementation of sound security and business practices. Successful risk management incorporates these security dependencies through technical oversight, business safeguards, and legal compliance established in contracts and service level agreements (SLAs).



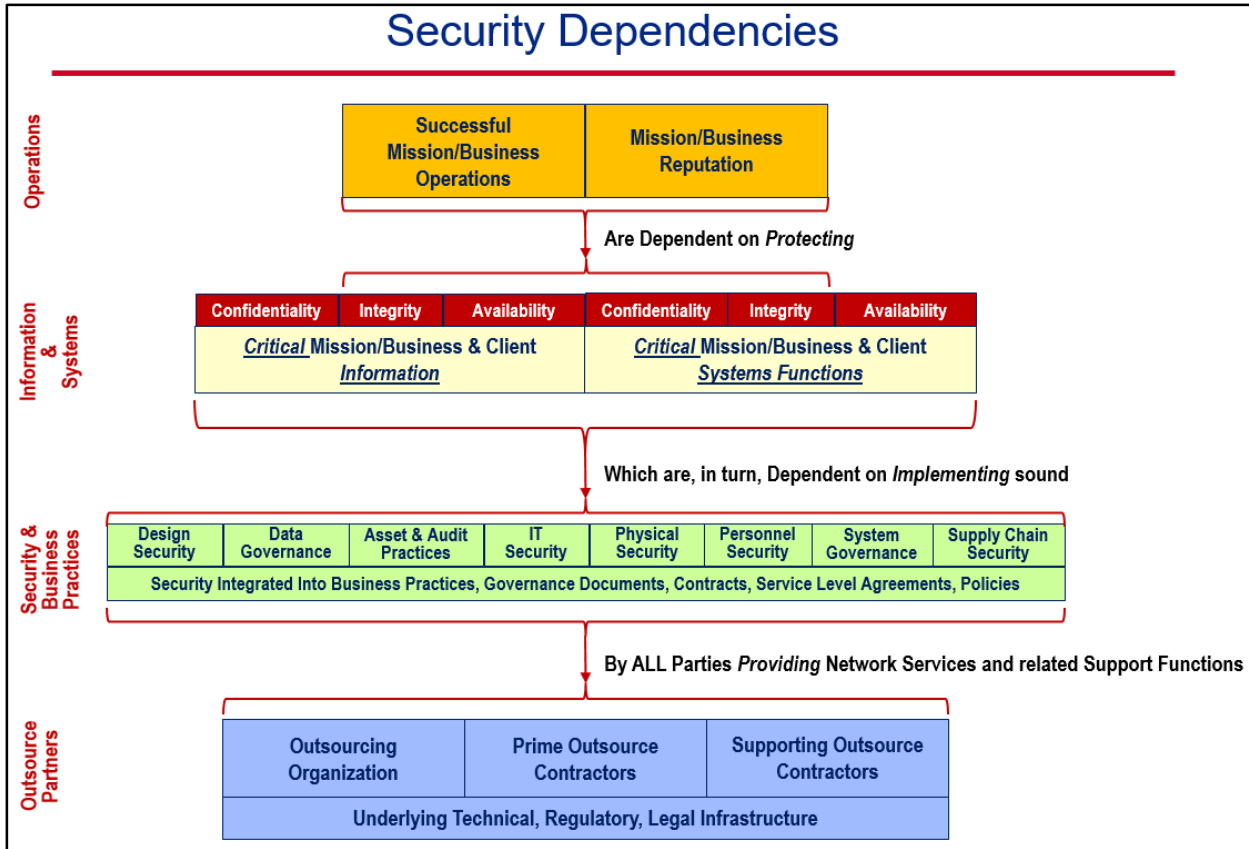


Figure 3: Security Dependencies When Extending Security Boundaries Due to Outsourcing

#### 1.4. ONSAT as a Decision Aid

ONSAT is a decision aid that brings risk-based information into the corporate decision-making process so that the benefits, financial costs, security risk cost, and business risk cost collectively inform critical network service outsourcing risk management decisions (Figure 4).

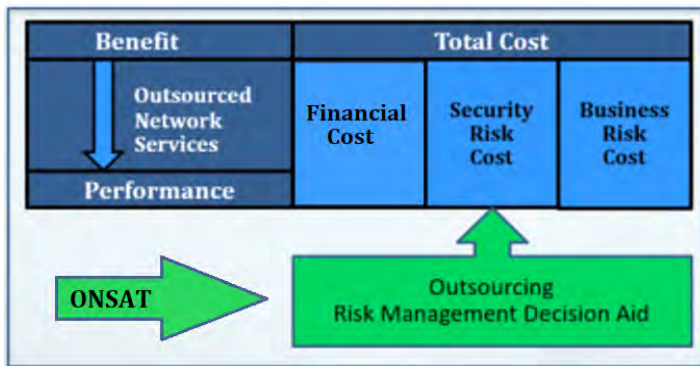


Figure 4: ONSAT Decision Aid for Determining Total Cost

Cost is typically defined by the initial dollars spent, but this definition does not take into account the total cost of ownership. Specifically, the Total Cost of Ownership is the sum of the Initial Cost of Implementation, plus the Cost of Operations and Maintenance, plus the Cost Associated with Risk. The Total Cost of Ownership lasts for the lifecycle of an outsourcing decision. (Figure 5, next page).

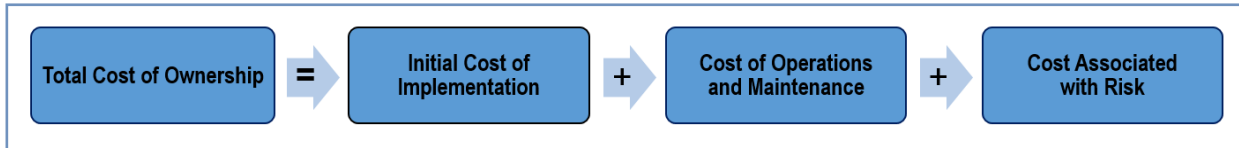


Figure 5: Total Cost of Ownership

ONSAT does not replace business and security assessments that are more robust or part of a formal certification program e.g. ISO/IEC 27001 Information Security Management. For larger organizations, robust assessments such as Service Organization Control (SOC) reports are a component of the best available evidence. For organizations of *all* sizes, ONSAT provides a common interface to security frameworks, best business practices, and financial cost to support risk management decisions without serving as a database for evidence or proprietary information (Figure 6).

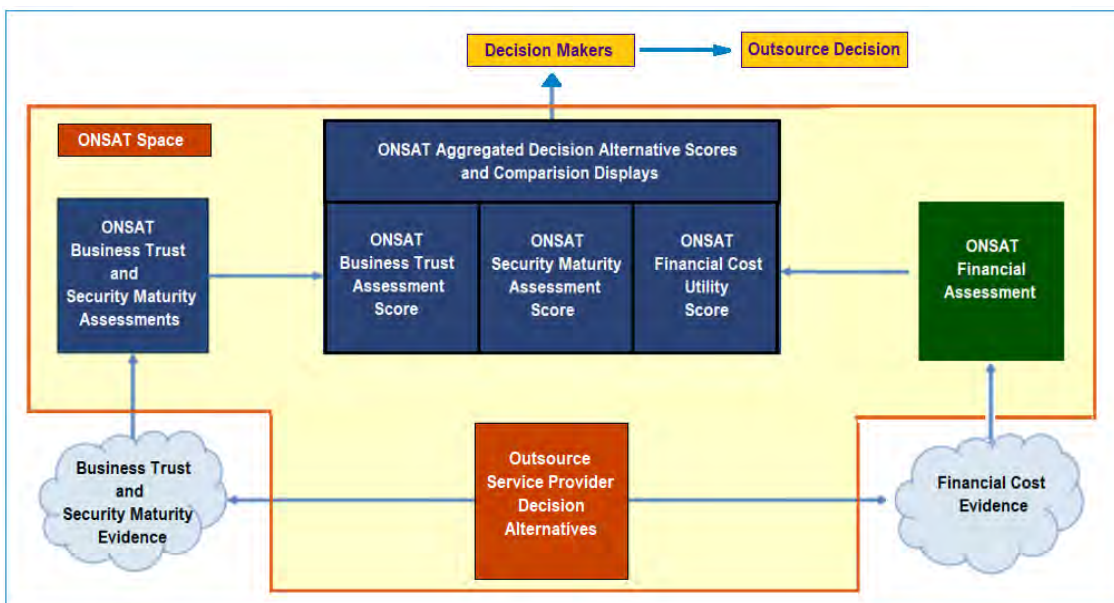


Figure 6: ONSAT Operating Space

ONSAT implements an analytic approach that uses the best available evidence to assess if, and how well, potential outsourcing partners and their supporting suppliers implement business and security practices critical to protecting the confidentiality, integrity, and availability of corporate and client mission and business critical information and functions. The assessor determines if and how well the organization implements business and security practices based on analysis of available evidence. Individual scoring is rolled up into overall scores for business trust, security maturity, and financial cost utility and displayed for informed decisions. To support outsourcing risk management decision processes, ONSAT displays aggregated and summarized results including reviews of individual partner organizations, and detailed comparative analysis of potential alternatives comprised of the outsourcing organization and combinations of a prime and / or a subcontractor (Figure 7, next page).



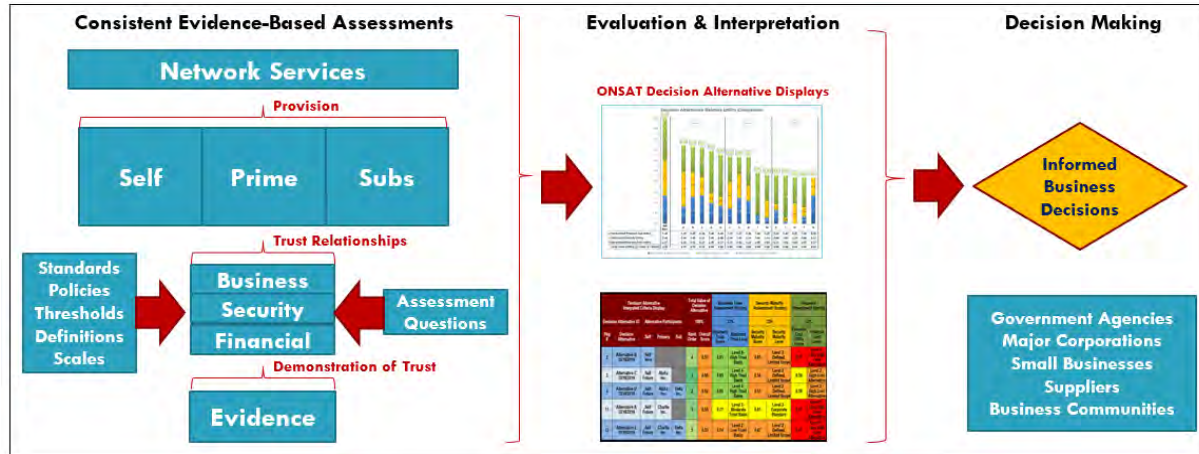


Figure 7: ONSAT Objectives: Total Cost Informed Decision Making Process

**The objectives of ONSAT are as follows:**

1. Provide a consistent approach for use by public and private organizations to determine their total risk picture for outsourcing network services and to assess alternative courses of action for risk management,
2. Assist Private Industry and Government Agencies Improve Their Understanding of the Trustworthiness of Potential Outsource Partners,
3. Enable linkage across business and technical aspects of risk management,
4. Ask The Right Questions about Business Trustworthiness of Outsource Partners,
5. Ask The Right Questions about Outsource Partner’s Maturity of Information Security Practices,
6. Assist in Translating Available Evidence into Outsourcing Decision-Support Information,
7. Encourage Consistent Evidence-Based Assessments,
8. Encourage Maturing of Evidence, Understanding, and Trust Over Time,
9. Encourage Formation of Communities of Trust and Information Sharing for example the management of access via Trust Federations<sup>8</sup>,
10. Reduce Company and Organizational Risks Through Improved Evidence, Assessments, Trend Analysis and increase awareness of the “cost” component of security and business risk.

**1.5. The Component of Risk Addressed by ONSAT**

If an organization does not properly manage risk, they may incur substantial losses because the focus of their mitigation efforts is in the wrong areas. The below diagram (Figure 8, next page) is a pictorial representation of the components of risk. To conduct a full risk analysis, all the components of Threat, Vulnerability, and Impact are considered. From this perspective, ONSAT does not incorporate a classic risk model. Specifically, ONSAT does not directly measure the effectiveness of defensive measures in mitigating risk. An assessor uses ONSAT to determine if, and how well, all the parties involved in an outsourced network service partnership are implementing both security and business practices needed to manage the risks and as such is assessing the resultant “net effect”. The underlying assumption is that

<sup>8</sup> NISTIR 8149 Developing Trust Frameworks to Support Identity Federations. Retrieved from: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf>

well-implemented defensive measures (business and security) will be more effective than defense measures that are not implemented or poorly implemented.

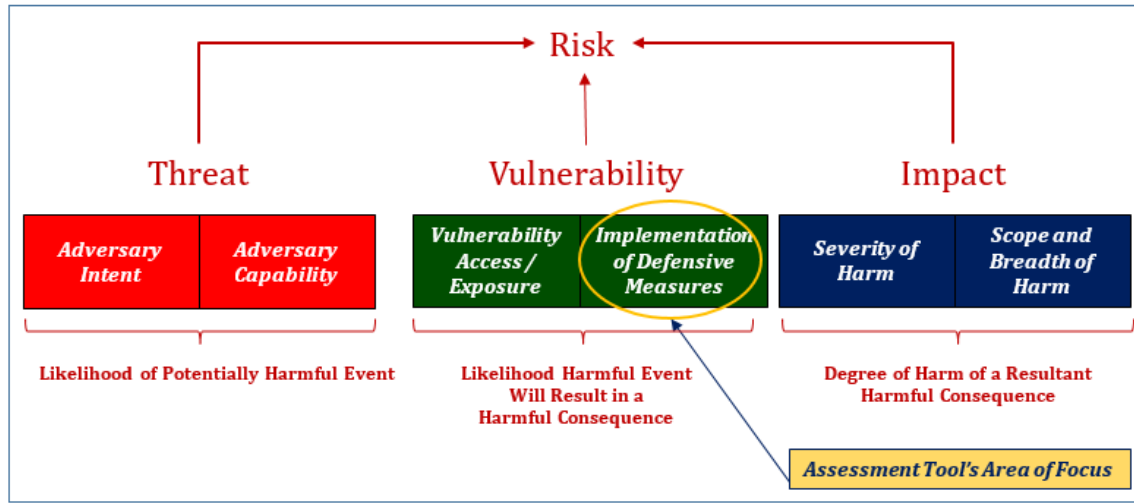


Figure 8: Components of Risk Addressed by ONSAT

In the diagram:

- **Threat** is dependent on *Adversary Intent* and *Adversary Capability*.
- **Vulnerability** is dependent upon the *Access and Exposure* of system vulnerabilities to exploitation and the *Maturity of Defensive Measures* to mitigate potential exploitations, and
- **Impact** is dependent upon the *Severity of Harm* of a single incident and *Scope and Breadth of Harm* that defines how widespread and how long that Level of Impact will affect the corporate mission or business objectives.
- **Risk** is the potential that a threat will exploit a vulnerability to cause harm or impact to an organization.
- **Risk management** often involves determining those risks with the greatest impact and greatest probability of occurring, and handling those first.

*Note:* ONSAT assumes that corporate decision-makers understand the potential threat environment in which they operate as well as the degree of harm that can result to their current and future business interests because of a successful security breach.

## 2.0 Inside ONSAT

### 2.1 Overview of ONSAT Architecture and Components

ONSAT's architecture underpins the assessment's analytic approach. The major components of ONSAT's architecture include Business and Security Frameworks, Business Trust and Security Maturity Categories, Business Trust and Security Maturity Assessments and associated scales, Financial Cost Utility Assessment and associated scale, displays of individual provider results, and displays of aggregated decision alternatives. ONSAT components have corresponding tabs in the tool and are generally arranged in order of operation.

## 2.1.1 Business and Security Frameworks

ONSAT employs business foreign investment review practices and provides a common interface to established security frameworks and guidance to support evidence-based risk management decisions. These frameworks form the foundation of ONSAT's architecture.

### 2.1.1.1 Business Investment Framework

Objectives of ONSAT include improving companies and organizations' understanding of the trustworthiness of potential outsourcing partners through evidence-based assessments. The ONSAT Business Assessment aligns with the information business investors are required to provide in a Joint Voluntary Notice (JVN), a formal filing notification under The Committee on Foreign Investment in the United States (CFIUS) process.

- CFIUS was established as an interagency committee in 1975 under executive order by President Ford to review certain transactions involving foreign investment in the United States, in order to determine their effect on the National Security of the United States. CFIUS was most recently modified with the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). Fully effective February 13, 2020, FIRRMA strengthened and broadened CFIUS authorities to include certain non-controlling foreign investment in specific types of U.S. businesses involved in critical technology, critical infrastructure, or collection of sensitive personal data on U. S. citizens.<sup>9</sup>

Both the business assessment in ONSAT and the JVN convey information to experts in a standard format that can be reviewed and assessed for risk. ONSAT equates assessment scores to trust levels to inform decision making; CFIUS decision options can include conditions that mitigate identified risks<sup>10</sup>.

### 2.1.1.2 Security Frameworks and Standards

ONSAT aligns to ten established frameworks and standards with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)\* as the overarching standard. The individual frameworks listed below detail controls and processes that organizations should leverage to improve the security of their outsourced network services. As an integrated set, these frameworks serve as the foundation to define the critical information necessary to conduct the security assessment. To anchor these controls and processes into ONSAT, each individual framework within the set is mapped to ONSAT's security categories. For further details on how the security frameworks and guidance are mapped to ONSAT's security categories, including an example of the mapping, please refer to [Annex 1. Mapping of Security Frameworks and Guidance](#). ONSAT security categories are mapped to the below security frameworks and standards; current versions are noted where applicable.

- \*NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014 (<https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>) (Current Version 1.1, April 16, 2018)<sup>11</sup>

<sup>9</sup> <https://crsreports.congress.gov/product/pdf/IF/IF10952>

<sup>10</sup> <https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview>

<sup>11</sup> <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

- Cloud Security Alliance - Consensus Assessments Initiative Questionnaire, Version 1.1, September 1, 2011 (<https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v1-1/>) (Current Version 3.1, November 15, 2019)<sup>12</sup>
- Department of Defense (DoD) Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), Cybersecurity Maturity Model Certification (CMMC) Version 0.7-Draft, December 6, 2019<sup>13</sup>
- International Standard ISO/IEC 27001:2013 [Information Technology - Security Techniques - Information Security Management Systems - Requirements] October 1, 2013<sup>14</sup>
- NIST Baldrige Cybersecurity Excellence Builder, Version 1.0, September 15, 2016 (Version 1.1, 2019)<sup>15</sup>
- NIST Special Publication (SP) 800-160 Volume 2- Developing Cyber Resilient Systems: A Systems Security Engineering Approach, November 2019<sup>16</sup>
  - Incorporates MITRE's Cyber Resiliency Engineering Framework (CREF) September 2011
- NIST Special Publication (SP) 800-161 [Supply Chain Risk Management Practices for Federal Information Systems and Organizations] [NIST SP 800-161] April 2015<sup>17</sup>
- NIST Special Publication (SP) 800-53 Rev 4 [ Security and Privacy Controls for Federal Information Systems and Organizations] [NIST SP 800-53r4] April 2013<sup>18</sup>
- Software Engineering Institute (SEI) Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector, [CMU/SEI-2012-SR-004] July 2012<sup>19</sup>
- Software Engineering Institute (SEI) Common Sense Guide to Mitigating Insider Threats 4th Edition [CMU/SEI-2012-TR-012] December 2012<sup>20</sup>

## 2.1.2 Business Trust and Security Maturity Categories

The Business Trust and Security Maturity Categories are the next layer in ONSAT's architecture. Both sets of categories define the types of information needed by an organization to verify the trustworthiness of potential outsource partners. The categories serve as a backdrop against which Business Trust and Security Maturity Assessments are structured and potential partners are assessed and scored.

### 2.1.2.1 Business Trust Categories

ONSAT's eight Business Trust Categories cover distinct vectors of business trust (Figure 9). A description of the information expected across the categories is below:

- Categories A and B: service provider information,
- Categories C and D: services required from a characteristics and a performance perspective,
- Category E: information about how a potential or existing service provider addresses restrictions related to Non-U.S. involvement in provision of the required services,

<sup>12</sup> <https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/>

<sup>13</sup> [https://www.acq.osd.mil/cmmc/docs/CMMC\\_Version0.7\\_UpdatedCompiledDeliverable\\_20191209.pdf](https://www.acq.osd.mil/cmmc/docs/CMMC_Version0.7_UpdatedCompiledDeliverable_20191209.pdf)

<sup>14</sup> <https://www.iso.org/standard/54534.html>

<sup>15</sup> <https://www.nist.gov/system/files/documents/2019/03/24/baldrige-cybersecurity-excellence-builder-v1.1.pdf>

<sup>16</sup> <https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final>

<sup>17</sup> <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf>

<sup>18</sup> <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

<sup>19</sup> [https://resources.sei.cmu.edu/asset\\_files/SpecialReport/2012\\_003\\_001\\_28137.pdf](https://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf)

<sup>20</sup> [https://resources.sei.cmu.edu/asset\\_files/TechnicalReport/2012\\_005\\_001\\_34033.pdf](https://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf)

- Categories F, G, and H: information on service provider(s) business’ stability, relationships with special interest groups, relevant claims, general reputation, and direct historical trust experience.

Cat ID	Business Categories	Categories Descriptions
A	Service Provider Identification	General Business Identification and Location and Size of Operation Information
B	Service Provider Profile	General Description of the Companies, Locations, and Personnel that Will Be Providing the Services
C	Major Specific Characteristics Associated with Services Provided	Description of Provider’s Ability to satisfy the Characteristics of services called for in provision of services
D	Major Specific Requirements Associated with Services Provided	Description of Provider’s Ability to satisfy the major performance, technical, interface, security, and subcontractor pass-thru Requirements and Constraints Associated called for in provision of services
E	Non-U.S. Involvement and Control Associated with Services Provided	Description of Provider’s Ability to satisfy restrictions on Non-U.S. involvement/control in provision of services including reporting and review requirements
F	Business Owner Profile	General Business Information including Incorporation, Ownership, Primary Managing Officers, Net Worth, and Volume/Value of Business annually
G	Business Relationships, Relevant Claims, Judgements, and Reportable Cybersecurity Incidents	General Information about Relationships with U.S. and Non-U.S. Governments Special Interest groups, as well, as Relevant claims, judgements and reportable cybersecurity incidents
H	General Reputation and Historical Trust Relationship	General Reputation and Direct Historical Trust Relationship Information Influencing Service Provision Decision

Figure 9: Business Trust Categories

### 2.1.2.2 Security Maturity Categories

ONSAT’s Security Maturity Categories are comprised of eighteen security practice categories further grouped into eight Functional Security Areas (Figure 10). ONSAT’s eighteen security categories are derived from the set of security frameworks and standards previously described in 2.1.1. The mapping of Security Maturity Categories to controls in security frameworks and standards promotes a common interface and evidence trail between the security standards and ONSAT.

Functional Security Areas	Cat #	Security Categories
System Design	1	Mission and Security Requirements, Roles, Responsibilities and Policies
	2	System Performance, Resiliency, and Security Architecture and Design Practices
Data Governance	3	Communication Path, Data Flow, and Data Governance Policies and Practices
Assets and Audit	4	Asset Inventory and Audit Management Practices
Information System Security	5	Authentication and Access Control Practices
	6	Network Segmentation Practices
	7	Data Confidentiality, Integrity and Availability Protection Practices
	8	Vulnerability and Resilience Management Practices
	9	System Maintenance and Repairs Practices
	10	Incident Detection and Response Practices
	11	Consequence / Impact Recovery Practices
	12	Configuration Management Practices
Physical Security	13	Physical / Facilities Security Policies and Practices
Personnel Security	14	Personnel Security Policies, Awareness, and Training
System Governance	15	Performance Management Practices
	16	Governance, Risk and Compliance (GRC) Management Practices
Supply Chain	17	HW/SW Asset Integrity Protection Practices
	18	Supplier Documentation and Vetting Policy and Practices

Figure 10: Security Maturity Categories



### 2.1.3 Business Trust and Security Maturity Assessments and Associated Scales

The Business Trust and Security Maturity Assessments are critical components of the analytic approach to aid in the evaluation of potential and existing outsource partners. The assessment questions in the ONSAT tool support the analytical approach to evaluating the trustworthiness of existing or new outsource partners using the best available evidence. Both assessments can be tailored based on the type of industry, size of organization or specific needs of the services being provided. The assessment questions assess not only the prime provider(s) but also drill down to assess additional providers including sub-contracted providers as documented in the *Service Provider Definition* Tab. To ensure applicability to a diverse user base, ONSAT does not provide the option to store evidence or documents. The Business Trust Assessment uses two scales, the Business Information Verification Scale and the Business Information Trust Basis Scale; the Security Assessment uses the Security Maturity scale.

#### 2.1.3.1 Business Trust Assessment Questions

The Business Trust Assessment consists of seventy-five questions across the eight Business Categories. The number of questions in each category varies. The first thirty questions are verification questions covered in Categories A, B, and C (see Figure 11). The verification questions evaluate factual business information. A complete list of business questions is available in [Annex 2. Business Assessment](#).

<b>A</b>	<b>SERVICE PROVIDER IDENTIFICATION (Questions 1-8)</b>
1	Company/Business name
2	Company Primary Service Provider Location
3	Company Primary Service Provider Business Contact
4	Company Primary Service Provider Security Contact
<b>B</b>	<b>BUSINESS OWNER PROFILE (Questions 9-21)</b>
9	Publicly or privately held company
12	Type of legal entity and state(s) / nations(s) of incorporation / place of legal organization
13	Place of Incorporation / Legal Organization
15	Name of the holding or parent company(s); include ultimate holding or parent company regardless of levels in between your company and parent company
16	Name and relationship with subsidiary and owned businesses
17	Alternative Doing Business As (DBA) Names
<b>C</b>	<b>SERVICE PROVIDER PROFILE (Questions 22-30)</b>
22	Name and description of services and products to be provided
23	Service and Product delivery model
24	Providers Participating in Producing / Providing Products / Services
25	Primary Location of Production / Provision of Products / Services
26	Backup Locations of Production / Provision of Products / Services
27	Primary Providers Participating in Providing Data Processing, Storage, and Transmittal Services
28	Primary Locations of Provision of Data Processing, Storage, and Transmittal Services
29	Backup Locations of Provision of Data Processing, Storage, and Transmittal Services

Figure 11: Example Business Trust Assessment Provider Verification Questions

The remaining forty-five questions in the Business Trust Assessment are questions covering categories D, E, F, G, and H (see Figure 12). These assessment questions assess the ability of the potential or existing provider to perform the needed services while satisfying legal, technical, and performance specifications.

<b>D</b>	<b>MAJOR CHARACTERISTICS OF SERVICE(S) TO BE PROVIDED (Questions 31-35)</b>
32	Assessment of Ability to Provide Support to Protect Major Business Functions Affected if Service is Not Provided as Specified
33	Assessment of Ability to Protect Identified Sensitive Data Associated with this Service
34	Assessment of Ability to Satisfy Major Legal Requirements / Issues / Exposure Associated with Service
<b>E</b>	<b>MAJOR SPECIFIC REQUIREMENTS OF SERVICES TO BE PROVIDED (Questions 36-50)</b>
36	Assessment of Ability to Satisfy Major Service Level Agreement Performance Specification / Requirements
37	Assessment of Ability to Satisfy Major Technical Implementation Specifications / Requirements
40	Assessment of Ability to Satisfy Major Data Confidentiality / Privacy Specifications / Requirements
42	Assessment of Ability to Satisfy Major Data Availability Specifications / Requirements
43	Assessment of Ability to Satisfy Major System / Network Access Specifications / Requirements
45	Assessment of Ability to Satisfy Major System / Network Availability Specifications / Requirements
46	Assessment of Ability to Satisfy Major Physical Access and Privilege Specifications / Requirements
48	Assessment of Ability to Satisfy Major Personnel Access and Privilege Specifications / Requirements
50	Assessment of Ability to Satisfy Major Supply Chain Security and Delivery Specifications / Requirements
51	Assessment of Ability to Satisfy Major Subcontractor Provider Specification / Requirements
<b>F</b>	<b>NON-U.S. INVOLVMENT AND CONTROL ASSOCIATED WITH SERVICES PROVIDED (Questions 52-62)</b>
52	Assessment of Ability to Adhere to Restrictions on Non-U.S. Involvement and Control in Provision of Services
54	Assessment of Ability to Adhere to Reporting and Review Requirements When There Are Changes to the Service Providers, Delivery Model, Contracts, or Special Security Accommodations to Assure Continued Compliance.
59	Assessment of Impact on Trust Basis of Other Non-U.S. Parties Providing the Services and Products
61	Identification and Assessment of Non-U.S. Parties Providing Associated Data Processing, Storage, and Transmittal Services
<b>G</b>	<b>BUSINESS RELATIONSHIPS, RELEVANT CLAIMS, JUDGEMENTS, AND REPORTABLE CYBERSECURITY INCIDENTS (Questions 63-67)</b>
63	Assessment of business relationships, contracts, or grants with the U.S. Government
64	Assessment of business relationships, contracts, or grants with Non-U.S. Governments
66	Assessment of Significant current or past legal claims or judgements that can affect the provision of these services
<b>H</b>	<b>GENERAL REPUTATION AND HISTORICAL TRUST RELATIONSHIP (Questions 68-75)</b>
68	Assessment of General Historical Trust Reputation
69	Assessment of Direct Historical Trust Relationships

Figure 12: Example Business Assessment Provider Ability Questions

### 2.1.3.2 Business Assessment: Information Verification Scale

The Business Information Verification Scale is a binary scale of the aggregated measure of "Verified or Unverified" business information. Based on the best available evidence, an assessor assigns a value to each of the thirty verification questions using the Business Information Verification Scale (Figure 13). The Business Information Verification Scale includes levels for "Insufficient Evidence" and "Not Applicable." The scale level of "Insufficient Evidence" is assigned when the information being assessed is questionable and/or cannot substantiate trustworthiness of the partner. The scale level of "Not Applicable" is assigned when the question does not apply to the outsourcing scenario or defined problem. For example, if an outsourcing organization has an internal policy or contractual obligation requiring it to retain a portion of the service in house, then certain questions in the assessment are likely not applicable.

Level ID	Business Information Verification Level	Defined Values
0	Insufficient Evidence	0.00
1	Level 1 - Unverified Information	0.20
5	Level 5 - Verified Information	0.95
6	Not Applicable	

Figure 13: Business Information Verification Scale

### 2.1.3.3 Business Trust Assessment: Information Trust Basis Scale

The Information Trust Basis Scale is an aggregated measure of the "Trust Basis." Trust Basis is a function of the level of confidence in the completeness and the reliability of the available information. Based on the best available evidence, an assessor assigns a value to each question using the Business Information Trust Basis Scale (Figure 14). The Business Information Trust Basis Scale has five-levels with defined values and an associated color scheme, and includes additional levels for "Insufficient Evidence" and "Not Applicable". Information completeness and information reliability should be considered as individual components when determining the appropriate level from the Business Trust Basis Scale. Although not incorporated into this version of ONSAT, separate scales for information completeness and information reliability support analytic objectivity and align with the evidence-based approach embedded in ONSAT.

Level ID	Business Information Trust Level	Defined Values
0	Insufficient Evidence	0.00
1	Level 1 - Very Low Trust Basis	0.20
2	Level 2 - Low Trust Basis	0.50
3	Level 3 - Moderate Trust Basis	0.75
4	Level 4 - High Trust Basis	0.85
5	Level 5 - Very High Trust Basis	0.95
6	Not Applicable	

Figure 14: Business Information Trust Basis Scale

### 2.1.3.4 Security Maturity Assessment Questions

The Security Maturity Assessment consists of ninety questions across eighteen categories (Figure 15). The five questions per category reflect a broad summary of issues associated with the category. Refer to the mapped security frameworks for a more detailed definition of characteristics and controls associated with each security category. To address one of the current concerns of supply chain risk management related to outsourcing of services, the fifth question in every category emphasizes the critical need for linkage across business and technical aspects of risk management. A complete list of security questions is available in [Annex 3. Security Assessment](#).



<b>1</b>	<b>RRR</b>	<b>1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]</b>
4	RRR - 1.4	4) Does corporate management maintain oversight to ensure Mission/Business security requirements are in place as well as authorizing their implementation as well as holding responsible entities accountable?
5	RRR - 1.5	5) Are Mission/Business security requirements incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>2</b>	<b>SDI</b>	<b>2) System Performance, Resiliency, and Security Architecture and Design Practices [System Design]</b>
3	SDI - 2.3	3) Are functions for monitoring, reporting, and responding to anomalous performance, resiliency, and security behaviors tested and exercised prior to implementation and periodically during operations?
<b>3</b>	<b>DFG</b>	<b>3) Communication Path, Data Flow, and Data Governance Policies and Practices [Data Governance]</b>
5	DFG - 3.5	5) Are Communication Path, Data Flow, and Data Governance Policies and Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>5</b>	<b>AAC</b>	<b>5) Authentication and Access Control Practices [Info. Sys.Security]</b>
3	AAC - 5.3	3) Are the processes for assessing and allowing access and privilege based on credentials documented, incorporated, and trained? Do these processes assure that only authorized individuals and entities have access and privilege to Mission/Business Critical Information, Services, and Assets?
<b>7</b>	<b>CIA</b>	<b>7) Data Confidentiality, Integrity and Availability Protection Practices [Info. Sys.Security]</b>
2	CIA - 7.2	2) Are Mission/Business Critical Information, Functions, Services, and Assets Identified and Documented to support effective positive and negative access control through Data Confidentiality, Integrity, and Availability Protection Practices?
<b>10</b>	<b>SMR</b>	<b>10) System Maintenance and Repairs Practices [Info. Sys.Security]</b>
2	SMR - 10.2	2) Are System Maintenance and Repair personnel identified and vetted, and are repair procedures and implementations documented, reviewed, inspected, and tested to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
<b>12</b>	<b>CIR</b>	<b>12) Consequence / Impact Recovery Policies and Practices [Info. Sys.Security]</b>
2	CIR - 12.2	2) Are the direct technical and procedural effects of failures, accidents, natural disasters, and intentional attacks documented and mapped to their broader operational effects on the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets and ultimately to Mission/Business operations?
<b>14</b>	<b>PSP</b>	<b>14) Personnel Security Policies, Awareness, and Training [Personnel Security]</b>
3	PSP - 14.3	3) Are Personnel Security Policies and Practices assessed, personnel trained, and procedures exercised to assure the identity and trustworthiness of employees, contractors, maintenance and service personnel, and visitors with physical or logical access to Mission/Business Critical Information, Functions, Services, and Assets?
<b>16</b>	<b>GRC</b>	<b>16) Governance, Risk, and Compliance (GRC) Management Practices [System Governance]</b>
3	GRC - 16.3	3) Are Governance, Risk, and Compliance (GRC) policies, requirements, and obligations and their implementation effectively incorporated into the decision-making culture and management practices throughout the organization?
<b>18</b>	<b>SDV</b>	<b>18) Supplier Documentation and Vetting Policy and Practices [Supply Chain]</b>
2	SDV - 18.2	2) Are Supplier Documentation and Vetting Policy and Practices documented, personnel trained, and procedures exercised to assure the integrity of products and services provided by this Supplier to preserve the Confidentiality, Integrity, and Availability of Mission/Critical Information, Functions, Services, and Assets?
5	SDV - 18.5	5) Are Supplier Documentation and Vetting Policy and Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?

Figure 15: Example Security Assessment Questions

### 2.1.3.5 Security Assessment: Security Maturity Scale

The Security Maturity Scale is an aggregated measure of the "maturity of implemented security practices." Based on the best available evidence, an assessor assigns a value to each question using the Security Maturity Scale (Figure 16). Evaluation verbs are incorporated in each question to aid analysis of available evidence and to prompt the assessor to ask if and how well the provider integrates their security and business practices. The Security Maturity Scale has five levels with defined values and

associated color scheme, and includes additional levels for “Insufficient Evidence” and “Not Applicable.” Full descriptions for each level are available in the *Scale Format Look Up* Tab.

Level ID	Security Maturity Level	Defined Values
0	Insufficient Evidence	0.00
1	Level 1 - Undefined, Undocumented	0.20
2	Level 2 - Defined, Limited Scope	0.50
3	Level 3 - Corporate Standard	0.75
4	Level 4 - Quantitatively Managed	0.85
5	Level 5 - Corporate Optimization	0.95
6	Not Applicable	

Figure 16: Security Maturity Scale

### 2.1.4 Financial Assessment and Associated Scale

ONSAT addresses a major gap in supply chain risk management by bringing both the cost of business risk and security risk, and the critical link between these two factors into the outsourcing decision process. ONSAT also incorporates the financial cost as a component of the analytic approach using the financial assessment. Similar to the Business Trust and Security Maturity Assessments, the Financial Cost Utility Assessment leverages the best available evidence. The Financial Cost Utility Assessment is unique compared to the other two assessments in that it is not driven by a set of categories and questions.

The Financial Cost Utility Assessment uses a template to capture the entire service cost for each provider based on the whether the defined role of the provider in the decision alternatives is the outsourcing organization, a prime, or a sub acting as a prime. ONSAT assigns each decision alternative a cost utility value based on the entire service cost as a percentage of the maximum financial reference (maximum budget allotted). The Financial Assessment Scale (Figure 17) is a measure of the "Utility Value of the Cost" of implementation based on the user-defined maximum budget for the total cost of provided service and the available evidence entered by the assessor(s).

Level ID	Financial Cost Utility Level	Defined Values
0	Over Budget	0.00
1	Level 1 - Very High Cost Alternative	0.10
2	Level 2 - High Cost Alternative	0.20
3	Level 3 - Moderate Cost Alternative	0.30
4	Level 4 - Low Cost Alternative	0.40
5	Level 5 - Very Low Cost Alternative	1.00
6	No Cost	

Figure 17: Financial Assessment Scale: Cost Utility Value

The Range of the Financial Cost Utility Value (preference) goes from 0.00 to 1.00 where 1.00 is the best case and 0.00 is the worst case. The utility value is relative to a user-defined maximum budget where the worst case (Utility = 0.00) is a cost that is equal to or greater than the maximum budget, and the best case (1.00) is no cost. The monetary cost and the utility values are inverted relative to each other

(Figure 17A). As the cost increases, the utility value decreases; as the cost decreases the utility value increase i.e. [Best Case: (\$0.00, Utility 1.00); Worst Case: (\$ Max Budget, Utility 0.00)].

$$\text{Financial Cost Utility} = \frac{(\$ \text{Max Budget} - \$ \text{Cost of Alternative})}{\$ \text{Max Budget}}$$

Figure 17A: Financial Cost Utility Formula

In the default Financial Cost Utility Scale, there is greater granularity to differentiate alternatives with higher costs approaching the maximum budget. For example, an alternative cost that is ten percent or less than the maximum budget is still regarded as *Very High Cost* while alternatives that are at least forty percent less than the maximum budget are considered *Very Low Cost*.

### 2.1.5 Display of Results and Integrated Decision Alternatives

ONSAT's analytic approach uses the best available evidence to assess the individual providers that comprise decision alternatives across the three decision criteria of business trust, security maturity, and financial cost utility. To further aid decision makers in understanding the trustworthiness of outsourcing partners, ONSAT provides a variety of displays and charts that enable scaled visualization of the decision alternatives and their embedded parts.

#### 2.1.5.1 Individual Provider Results and Summary Views

ONSAT displays results and summary views of the individual providers to enable review and comparative analysis. Full descriptions of the following displays using exemplar data are included in [Section 5.1 Individual Provider Results](#) and [Section 5.2 Summary Views](#).

- **Business Trust:** Provider Business Display, Provider Business Category Display, Business Summary
- **Security Maturity:** Provider Security Display, Provider Security Category Display, Security Summary
- **Financial Cost Utility:** Financial Summary

#### 2.1.5.2 Aggregated Results and Integrated Decision Alternative Displays

ONSAT's aggregated scoring and integrated alternative displays enable "rack and stack" analysis of the alternatives to guide the outsourcing decision and inform overall risk management for the organization. This is akin to a fully customizable menu of alternatives, which gives the user the ability to compare risk(s) of their selections. Full descriptions of the following displays using exemplar data are included in [Section 5.2 Aggregated Results and Integrated Decision Alternative Displays](#).

- Provider Integrated Display
- Decision Alternative Business Display
- Decision Alternative Security Display
- Decision Alternative Financial Display
- Decision Alternative Score Summary
- Decision Alternative Integrated Display
- Total Value Display (Ranked)
- Total Value Composite Chart

### 2.1.6 Overview of ONSAT Tabs

The current version of ONSAT is in a Microsoft Excel spreadsheet format comprised of fifty-two tabs grouped into seven color-coded sections (Figure 18). Each of the sections represents a major function or type of information within ONSAT. Each of the tabs within a section contains an input template, displays, or reference information. For example, the “Completed Example Tab” section contains twenty tabs prepopulated with exemplar data aligned with steps in the assessment and analysis of results. The order of ONSAT tabs in Figure 18 generally corresponds to the chronological process of conducting a full assessment.

There are two additional sections of tabs **not** included in the Overview of Tabs Figure:

- The “*Tool Adjustment Settings*” section contains eleven tabs that can be used to modify the content and/or weight of the questions and categories, the weight of the assessment types, and/or the scale values and format. The tabs begin with the *User Defined What If Values* Tab located behind the “Completed Example Tabs” section (see Annex 4: Tool Settings Adjustment).
- The “*Behind-the-scene*” tabs support functionality of ONSAT and should not be modified for basic use of the tool. These tabs are greyed out “hidden” and located at the end of all tool tabs.

Sections Color Coded by Function or Type of Information	List of Tabs in each Section	
Tool Information	<ul style="list-style-type: none"> <li>• Title Page</li> <li>• Version</li> </ul>	<ul style="list-style-type: none"> <li>• Table of Contents</li> <li>• Network Services &amp; Tool</li> </ul>
Outsourcing Scenario	<ul style="list-style-type: none"> <li>• Outsourced Service Definition</li> <li>• Service Provider Definition</li> </ul>	<ul style="list-style-type: none"> <li>• Decision Alternative Definition</li> </ul>
Default Tool Settings	<ul style="list-style-type: none"> <li>• Default Tool Settings</li> </ul>	
Business Assessment	<ul style="list-style-type: none"> <li>• Business Assessment</li> </ul>	
Security Assessment	<ul style="list-style-type: none"> <li>• Security Assessment</li> </ul>	
Financial Assessment	<ul style="list-style-type: none"> <li>• Financial Assessment</li> </ul>	
Business Display	<ul style="list-style-type: none"> <li>• Business Data Display</li> <li>• Provider Business Display</li> </ul>	<ul style="list-style-type: none"> <li>• Provider Business Category Display</li> <li>• Business Summary</li> </ul>
Security Display	<ul style="list-style-type: none"> <li>• Security Data Display</li> <li>• Provider Security Display</li> </ul>	<ul style="list-style-type: none"> <li>• Provider Security Category Display</li> <li>• Security Summary</li> </ul>
Financial Display	<ul style="list-style-type: none"> <li>• Financial Summary</li> </ul>	
Aggregated Results Display	<ul style="list-style-type: none"> <li>• Provider Integrated Display</li> <li>• Decision Alternative Business Display</li> <li>• Decision Alternative Security Display</li> <li>• Decision Alternative Financial Display</li> </ul>	<ul style="list-style-type: none"> <li>• Decision Alternative Score Summary</li> <li>• Decision Alternative Integrated Display</li> <li>• Total Value Display (Ranked)</li> <li>• Total Value Composite Chart</li> </ul>
Reference Look Up	<ul style="list-style-type: none"> <li>• Scale-Format Look up</li> <li>• Referenced Security Frameworks</li> </ul>	<ul style="list-style-type: none"> <li>• Security Frameworks Mapping</li> <li>• Compliance Mapping Reference</li> </ul>
Completed Example Tabs (pre-populated)	<ul style="list-style-type: none"> <li>• EX. Service Provider Definition</li> <li>• EX. Decision Alternative Definition</li> <li>• EX. Business Assessment</li> <li>• EX. Security Assessment</li> <li>• EX. Financial Assessment</li> <li>• EX. Provider Business Display</li> <li>• EX. Provider Business Category Display</li> <li>• EX. Business Summary</li> <li>• EX. Provider Security Display</li> <li>• EX. Provider Security Category Display</li> </ul>	<ul style="list-style-type: none"> <li>• EX. Security Summary</li> <li>• EX. Financial Summary</li> <li>• EX. Provider Integrated Display</li> <li>• EX. Decision Alternative Business Display</li> <li>• EX. Decision Alternative Security Display</li> <li>• EX. Decision Alternative Financial Display</li> <li>• EX. Decision Alternative Score Summary</li> <li>• EX. Decision Alternative Integrated Display</li> <li>• EX. Total Value Display (Ranked)</li> <li>• EX. Total Value Composite Chart</li> </ul>

Figure 18: Overview of ONSAT Tabs

### 3.0 Using ONSAT to Conduct an Assessment

As a decision aid, ONSAT elucidates the risk of network services outsourcing options. ONSAT assists in capturing and aggregating into overall comparison scores, individual insights associated with the following decision criteria:

- The Degree of Business Trust of Each Decision Alternative
- The Degree of Security Maturity Afforded Critical Information and Services of Each Decision Alternative
- The Financial Cost Utility Value of Each Decision Alternative

ONSAT contains three intertwined assessments as part of the overall assessment: Business Trust, Security Maturity and Financial Cost Utility. ONSAT affords users the ability to group one's own organization, prime contractor(s), and/or subcontractor(s) into various packages to form decision alternatives. The individual components of a decision alternative are assessed using consistent criteria and the results are rolled up into an Aggregated Total Score for comparison with other packages. In this manner, ONSAT helps to ensure that decision alternatives are equitably compared against each other.

To conduct an Overall Assessment, the user determines if and how well the organization implements business and security practices based on analysis of available evidence and aligns these outcomes with the associated financial cost for a total cost. Outlined below are the six major steps to conduct an overall assessment (Figure 19, next page). Each of the six steps builds upon the previous; and, therefore it is critical to not only complete the steps in order but to give due diligence to each step.

*This is Blank Space*

*This is Blank Space*



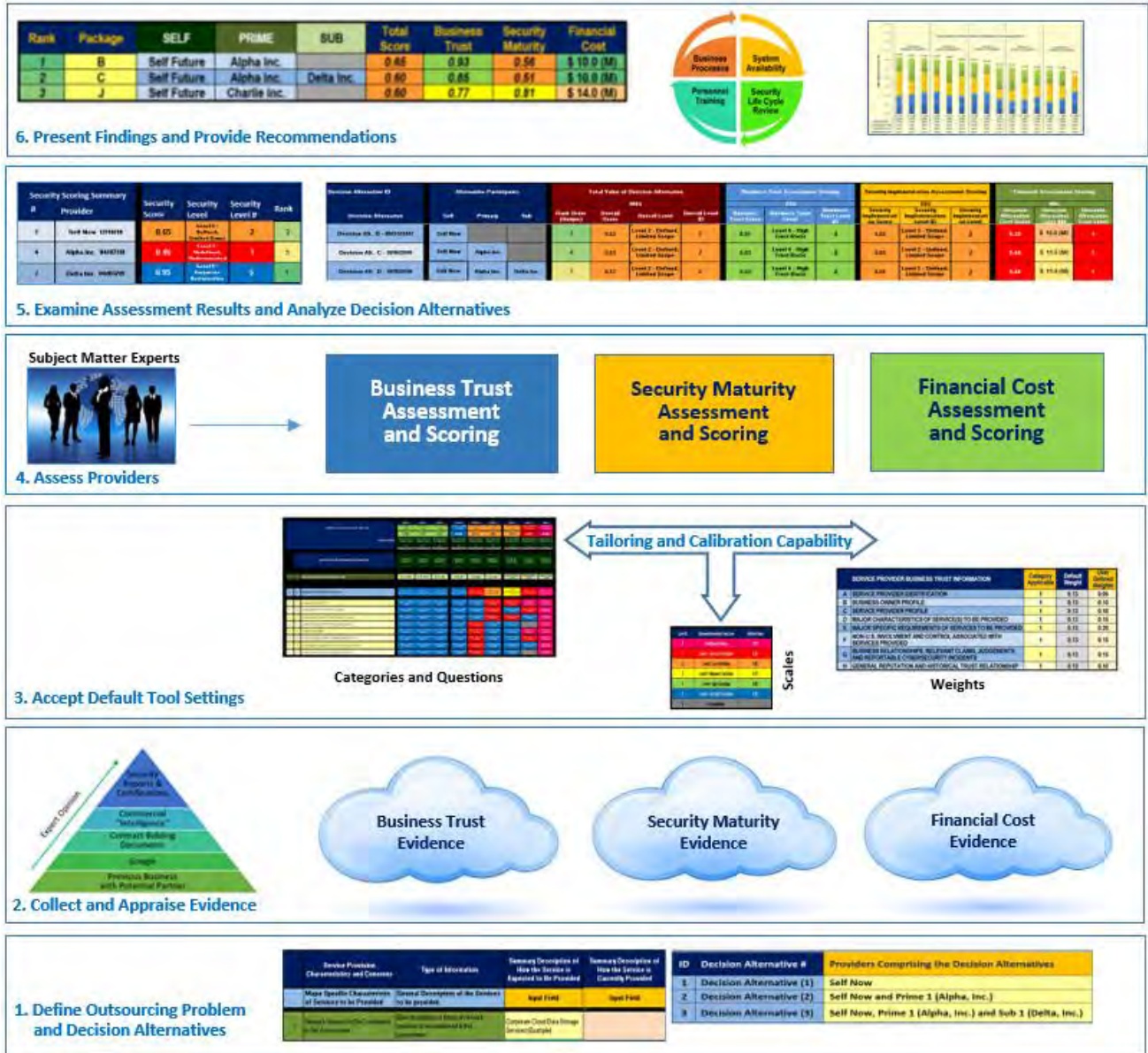


Figure 19: Six Major Steps for Conducting an Assessment

### 3.1 Step 1: Define Outsourcing Problem and Decision Alternatives

Before a user can determine if and how well an organization implements business and security practices, the user must first define the outsourcing problem and decision alternatives. The terms “Need Statement” or “Outsourcing Scenario” can be used in lieu of “Problem”.

There are three tabs associated with Step 1: Define the Outsourcing Problem and Decision Alternatives (Figure 20). Use the templates associated with each of the three tabs to define the network services being considered for outsourcing (Steps 1a), to define the network services requirements (Step 1b), to identify the individual providers up for consideration (Step 1c), and to document the combinations of providers that comprise each decision alternative (Step 1d). Each step and template builds upon the previous one. Similarly, the tool assessment and display functionality builds upon the information provided in Steps 1, 2 and 3.

Problem Definition Section	
Tab Name	Tab Description
Outsourced Service Definition	Template to Define the Network Services Considered for Outsourcing
Service Provider Definition	Template to Define the Set of Individual Providers Considered in the Assessment
Decision Alternative Definition	Template to Define the Combination of Providers for each Decision Alternative

Figure 20: Outsourcing Problem Definition and Decision Alternatives Tabs

### 3.1.1 Step 1a: Defining the Outsourced Network Service(s) Characteristics

Other tabs in the tool do not directly use information input in the *Outsourced Service Definition* Tab; however, the process of documenting the outsourcing problem aids clarity to the assessment and enables a common understanding across the organization of the issues and concerns intended to be resolved through outsourcing.

The *Outsourced Service Definition* Tab contains a template divided into two sections:

1. Major Specific **Characteristics** of Services to be Provided (top section)
2. Major Specific **Requirements** of Services to Be Provided (bottom section)

In the top section of this tab, define the **characteristics** of the network services considered for outsourcing using the template. Columns one through three are prepopulated to align with the eight characteristic areas; columns three and four are input fields (Figure 21, next page). Columns six through eight provide a cloud data storage service example and capability language prompts to support consistency in describing how the service is *expected* to be provided for each characteristic area (Figure 21A, next page).

- Column 1 identifies characteristic area number
- Column 2 identifies the name of the characteristic area
- Column 3 describes the type of information expected in this characteristic area
- Column 4 provides a summary description of how the service is *currently* provided
- Column 5 provides a summary description of how the service is *expected to be* provided
- Column 6 contains sample wording for *expected* delivery of Corporate Cloud Data Storage Services
- Columns 7 and 8 provide assessment capability prompts to aid consistency

Input in column four should identify the major business functions linked to this service, indicate whether there is sensitive data and/or access restrictions, list what events trigger a review, highlight major legal requirements or concerns, and specify “how” the services are *expected* to be provided. Distinction between how the service is *currently* provided (Column 4) and how the service is *expected* to be provided by an outsourcing partner (Column 5) should be easily discernible. Both input fields are of critical importance when outsourcing network services as they reinforce to the user that any delta between how services are *currently* provided and how services are *expected* to be provided must be accounted for by either the outsourcing organization and/or the outsourcing partner(s).

Area #	Service Provision Characteristics and Concerns	Type of Information	<==Columns 1 - 5==>	Description of How Service is <b>Currently</b> Provided	Description of How Service is <b>Expected to</b> Be Provided
	<b>MAJOR SPECIFIC CHARACTERISTICS OF SERVICES TO BE PROVIDED</b> (Example abbreviated, refer to tab).	General Description of the Services to be provided.		Input Field	Input Field
1	Network Services Considered in this Assessment	Brief description of network services considered in this assessment.			
2	Major Business Functions Affected if Service is Not Provided as Specified	Brief description of the major business functions that are dependent on the successful provision of this service....			
3	Sensitive Data Associated with this Service	Brief description or listing of the data associated with this Service that has special access/handling designations and requirements.			
4	Restrictions on Non-U.S. Involvement and Control...	Brief description of any Non-U.S. Involvement and Control issues...			
5	Special Security Arrangements / Agreements / Separation of Business and Data Accommodations to Satisfy Non-U.S. Involvement and Control Restrictions	Brief description of any Special Security Arrangements / Agreements / Separation of Business and Data Activity Accommodations needed to be satisfy in order to be in a position to provide these services.			
6	Reporting and Review Requirements When There Are Changes to the Service Providers, Delivery Model, Contracts, or Special Security Accommodations...	Brief description of any reporting and review requirements needed to assure that the provisions and agreements associated with this service continue to be complied with when there are changes.....			
7	Major Legal Requirements / Issues / Exposure Associated with this Service	Brief description of major legal requirements or issues associated with the provision of this service or outsourcing of this service.			
8	Defined Service Provision	Brief description of how the services will be provided.			

Figure 21: Major Specific Characteristics of Services to be Provided

<== Columns 6 - 8 ==>		
Example Summary Description of How the Service is Expected to Be Provided	Assessment Capability Language	Assessment Phrase
Example—abbreviated; refer to Tool Tab for full example	Aligned with the Characteristic Area	Specific to the Characteristic Area to Support Consistent Documentation
Corporate Cloud Data Storage Services (Example)	Assessment of Experience in Providing	Network Services to Be Considered in this Assessment
All business and security functions are dependent upon the data that is stored in the cloud. (Example)	Assessment of Ability to Provide Support	Protect Major Business Functions Affected if Service is Not Provided as Specified
HR Records, Customer Records, Internal and External Email Correspondence, Proprietary Research and Development Papers, Test Results, Designs, ...(Example)	Assessment of Ability to Protect	Identified Sensitive Data Associated with this Service
Due to Classified U.S. Government Contracts, all cloud data storage services, data storage locations, and personnel supporting the design, configuration, and management of data storage must be performed by U.S. Citizens...(Example)	Assessment of Ability to Adhere to	Restrictions on Non-U.S. Involvement and Control in Provision of Services
The U.S. Government contracts are managed as a separate division with a separate sub-network and data storage for data associated with these contracts. The data associated with these U.S. Government contracts.... (Example)	Assessment of Ability to Adhere to	Special Security Arrangements / Agreements / Separation of Business and Data Accommodations to Satisfy Non-U.S. Involvement and Control Restrictions
All changes in sub-contractors supporting this service need to be identified to the Contract Officer 3 months prior to execution of operational support on this data. The name and nationality of any Non-U.S. Person... (Example)	Assessment of Ability to Adhere to	Reporting and Review Requirements When There Are Changes to the Service Providers, Delivery Model, Contracts, or Special Security Accommodations...

Figure 21A: Major Specific Characteristics of Services to be Provided – Example and Assessment Prompts

### 3.1.2 Step 1b: Defining the Outsourced Network Service(s) Requirements

In the bottom section of this tab, *Major Specific Requirements of Services to be Provided*, define the major **requirements** of the network services considered for outsourcing using the template (Figure 22). Similar to the top template, there are eight columns. Columns one through three are prepopulated to align with the sixteen requirement areas; columns four and five are input fields. Columns six through eight (not shown) provide an example along with capability language prompts to support consistency in describing how to the service is *expected* to be provided for each requirement area.

- Column 1 identifies requirement area number
- Column 2 identifies the name of the requirement area
- Column 3 describes the type of information expected in this requirement area
- Column 4 provides a summary description of how the service is *currently* provided
- Column 5 provides a summary description of how the service is *expected to be* provided
- Column 6 contains sample wording for *expected* delivery of corporate cloud data storage services example
- Columns 7 and 8 provide assessment capability prompts to aid consistency

Input in column four should identify the major SLA performance specifications and requirements including technical and interface implementation, both data and network access, confidentiality,



integrity, and availability, as well as physical and personnel security and access requirements. Input in column four should also list supply chain specifications and requirements and document the specifications levied on the subcontractors including pass-through performance, technical, interface, and security requirements.

Distinction between how the service is *currently* provided (Column 3) and how the service is *expected* to be provided by an outsourcing partner (Column 4) should be easily discernible. Both input fields are of critical importance when outsourcing network services as they reinforce to the user that any delta between how services are *currently* provided and how services are *expected* to be provided must be accounted for by either the outsourcing organization and/or the outsourcing partner(s).

	Service Provision Requirements	Type of Information Expected in Input Field	Summary Description of How the Service is Expected to be Provided	Summary Description of How the Service is Currently Provided
	Major Specific Requirements of Services to be Provided	Major Performance, Technical, Interface, Security, and Subcontractor Pass-Thru Requirements and Constraints Associated with this Service.	Input Field	Input Field
9	Major Service Level Agreement Performance Specifications / Requirements	Brief listing of major SLA performance specifications and requirements.		
10	Major Technical Implementation Specifications / Requirements	Brief listing of major technical implementation specifications and requirements		
11	Major Interface Implementation Specifications / Requirements	Brief listing of major interface implementation specifications and requirements		
12	Major Data Access and Privilege Specifications / Requirements	Brief listing of major data access and privilege specification and requirements		
13	Major Data Confidentiality / Privacy Specifications / Requirements	Brief listing of major data confidentiality and privacy specifications and requirements		
14	Major Data Integrity Specifications / Requirements	Brief listing of major data integrity specifications and requirements		
15	Major Data Availability Specifications / Requirements	Brief listing of major data availability specifications and requirements (may be listed in SLA requirements)		
16	Major System / Network Access Specifications / Requirements	Brief listing of major system / network access specification and requirements.		
17	Major System / Network Integrity Specifications / Requirements	Brief listing of major system / network integrity specifications and requirements		
18	Major System / Network Availability Specifications / Requirements	Brief listing of major system / network availability specifications and requirements		
19	Major Physical Access and Privilege Specifications / Requirements	Brief listing of major physical access and privilege specifications and requirements		
20	Major Physical Security Specifications / Requirements	Brief listing of major physical security specifications and requirements		
21	Major Personnel Access and Privilege Specifications / Requirements	Brief listing of major personnel access and privilege specification and requirements		
22	Major Personnel Security Specifications / Requirements	Brief listing of major personnel security specifications and requirements		
23	Major Supply Chain Security and Delivery Specifications / Requirements	Brief listing of major supply chain and delivery specifications and requirements		
24	Major Subcontractor Provider Specification / Requirements	Brief listing of major subcontractor provider specifications and requirements including pass through performance, technical, interface, and security requirements.		

Figure 22: Major Specific Requirements of Services to be Provided

### 3.1.3 Step 1c: Defining the Potential Providers to be Assessed

Once the major characteristics and the major requirements of the network services considered for outsourcing are defined and documented, the next step is to identify and document the individual providers considered as potential outsourcing partners. Follow the guidelines set by your organization.

In this version of ONSAT, the number of potential or existing prime and sub partners for consideration is *limited to three each*. In future versions of ONSAT, this limitation should be removed. For all versions of ONSAT, there are three options for defining your organization as an outsourcing provider: Self Past, Self Now, and Self Future.

- A best practice is to have your organization’s previous assessment (Self Past) available for reference by including it as a provider in the *Service Provider Definition* Tab, but not as an option in the *Decision Alternative Definition* Tab.
- Remember, not outsourcing (keeping network service(s) in-house) is an option, so including the outsourcing organization (*Self Now*) as one of the potential providers is another best practice.
- *Self Future* is included as a provider and represents the portion of the work that the outsourcing organization would still perform under an outsourcing arrangement.

ONSAT’s key strengths include trend analysis and modeling. For example, identifying Self Past, Self Now, and Self Future as stand-alone decision alternatives enables an organization to determine their security and business competencies as well as their maturity gaps. As a follow-on to trend analysis, ONSAT is adept at modeling the effect of investments in, and modifications to, security and business practices.<sup>21</sup>

There are six fields of information required in the *Service Provider Definition* Tab (Figure 23). Refer to the *Example Service Provider Definition* Tab.

ID #	Specific Name	Date of Assessment	Entity Type	Short Title	Include in Assessment
1	Self Past	03/15/19	SELF	Self Past	2) No
2	Self Now	12/18/19	SELF	Self Now	1) Yes
3	Self Future	12/18/19	SELF	Self Future	1) Yes
4	Alpha Inc.	12/18/19	PRIME	Alpha Inc.	1) Yes
5	Bravo Inc.	12/18/19	PRIME	Bravo Inc.	1) Yes
6	Charlie Inc.	12/18/19	PRIME	Charlie Inc.	1) Yes
7	Delta Inc.	12/18/19	SUB	Delta Inc.	1) Yes
8	Echo Inc.	12/18/19	SUB	Echo Inc.	1) Yes
9	Foxtrot Inc.	12/18/19	SUB	Foxtrot Inc.	1) Yes

Figure 23: Example Service Provider Definition Tab

- **ID #:** in the tool, the ID # column is auto populated with 1 – 9 corresponding to the three providers for each entity type for a total of nine potential providers.
  - When a company or provider name is entered into the Specific Name field, ONSAT assigns the pre-generated ID# to this provider to be used throughout the assessment.
- **Specific Name:** name of the company or provider being assessed; specific name must be unique from other companies or organizations listed as a provider in the tool
- **Date of Assessment:** the date of the most recent assessment completed for this company or provider
- **Entity Type:** *Self, Prime or Sub* are used to define the role in the outsourcing decision for each provider.
  - Note: roles defined in the tool are not permanent i.e. depending on the project and specific requirements; the Prime can be the Sub, or the Sub the Prime.
- **Short Title:** a unique name that corresponds to the specific name and is short enough (recommend maximum of 15 characters) to accommodate field length in the tab.

<sup>21</sup> A companion document detailing the use of ONSAT in trend analysis and modeling for improved risk management is in the initial stage of planning.

- Short Title is used in all assessments and displays. When anonymity is a concern, the Short Title allows a means to restrict the full name of the company from displaying in all tabs of the tool, except in the Service Provider Definition Tab.
- **Include in Assessment:** indicates whether the provider will be included in a decision alternative.
  - In the example, Self Past is toggled to “No” to align with guidance that Self Past should not be included as a provider in the assessment unless you are performing trend analysis for your company or organization.

In the *Service Provider Definition* Tab, the template contains prepopulated entries for all three options for the outsourcing organization. To ensure ONSAT has the necessary data to compare providers and decision alternatives, data needs to be entered in the blank fields for prime(s) (1 to 3 primes) and subs (0 to 3) as applicable (Figure 24).

ID #	Specific Name	Date of Assessment	Entity Type	Short Title	Include in Assessment
1	Self Past		SELF	Self Past	1) Yes
2	Self Now		SELF	Self Now	1) Yes
3	Self Future		SELF	Self Future	1) Yes
4			PRIME		1) Yes
5			PRIME		1) Yes
6			PRIME		1) Yes
7			SUB		1) Yes
8			SUB		1) Yes
9			SUB		1) Yes

Figure 24: Service Provider Definition Starting Point

- Enter the **Date of Assessment** for *Self Past*, *Self Now*, and *Self Future*.
- In Rows ID #4 through ID #6:
  - Enter the **Specific Name**, **Date of Assessment**, and **Short Title** of the providers acting as Primes in the outsourcing scenario.
- In Rows ID #7 through ID #9:
  - Enter the **Specific Name**, **Date of Assessment**, and **Short Title** of the providers acting as Subs in the outsourcing scenario.
- For all providers’ ID #1 through ID #9:
  - Toggle to Yes or No in the Include in Assessment column to indicate whether the provider will be assessed (the default value is Yes).
  - Toggle *Self Past* to *No* to align with guidance that *Self Past* should not be included as a provider in the outsourcing decision.

As outsourcing providers are entered in the *Service Provider Definition* Tab, the **Short Title**, **Date of Assessment**, and **Entity Type** for each provider are replicated in the three *Assessment* Tabs. For any provider toggled to “Yes” in the **Include in Assessment** column, the **Short Title** of the provider is used to create the **Defined Service Providers** menu in the *Decision Alternative Definition* Tab.



### 3.1.4 Step 1d: Defining the Decision Alternatives (Combinations of Providers)

Once the individual providers are defined, the last part of Step 1 is to define the combinations of individual providers into packaged decision alternatives. In ONSAT, the number of decision alternatives is dependent on the number of outsourcing providers and their entity type as identified in Step 1.c. In many cases, decision alternatives for an outsourcing scenario will include multiple combinations of the outsourcing organization (Self), the outsourcing provider and a prime, and the outsourcing provider, a prime, and the prime's sub.

The prepopulated example in the *Example Decision Alternative Definition Tab* (Figure 25) is comprised of nine fields of information; four fields require data entry and the remaining are populated by ONSAT. Field Names below are bolded.

Date of Assessment	User Defined Specific Label	Entity Type Column			Selected Provider By Entity Type			Decision Alternative Specific Label (Defined Here)
		SELF	PRIME	SUB	SELF	PRIME	SUB	
	Choices=>	1,2,3	4,5,6	7,8,9				
12/18/2019	A	2			Self Now			Decision Alt. A - 12/18/2019
12/18/2019	B	3	4		Self Future	Alpha Inc.		Decision Alt. B - 12/18/2019
12/18/2019	C	3	4	7	Self Future	Alpha Inc.	Delta Inc.	Decision Alt. C - 12/18/2019
12/18/2019	D	3	4	8	Self Future	Alpha Inc.	Echo Inc.	Decision Alt. D - 12/18/2019
12/18/2019	E	3	4	9	Self Future	Alpha Inc.	Foxtrot Inc.	Decision Alt. E - 12/18/2019
12/18/2019	F	3	5		Self Future	Bravo Inc.		Decision Alt. F - 12/18/2019
12/18/2019	G	3	5	7	Self Future	Bravo Inc.	Delta Inc.	Decision Alt. G - 12/18/2019
12/18/2019	H	3	5	8	Self Future	Bravo Inc.	Echo Inc.	Decision Alt. H - 12/18/2019
12/18/2019		3	5	9	Self Future	Bravo Inc.	Foxtrot Inc.	Decision Alt. [ Self Future / Bravo Inc. / Foxtrot Inc. ] - 12/18/2019
12/18/2019		3	6		Self Future	Charlie Inc.		Decision Alt. [ Self Future / Charlie Inc. / _ ] - 12/18/2019
12/18/2019		3	6	7	Self Future	Charlie Inc.	Delta Inc.	Decision Alt. [ Self Future / Charlie Inc. / Delta Inc. ] - 12/18/2019
12/18/2019		3	6	8	Self Future	Charlie Inc.	Echo Inc.	Decision Alt. [ Self Future / Charlie Inc. / Echo Inc. ] - 12/18/2019
12/18/2019		3	6	9	Self Future	Charlie Inc.	Foxtrot Inc.	Decision Alt. [ Self Future / Charlie Inc. / Foxtrot Inc. ] - 12/18/2019
12/18/2019		3		7	Self Future		Delta Inc.	Decision Alt. [ Self Future / _ / Delta Inc. ] - 12/18/2019
12/18/2019		3		8	Self Future		Echo Inc.	Decision Alt. [ Self Future / _ / Echo Inc. ] - 12/18/2019

Figure 25: Example Decision Alternative Definition Tab

- Date of Assessment:** the date when a decision alternative (combination of Self, Prime, and Sub providers as a package) is assessed; entered by user.
  - It is important to distinguish this **Date of Assessment** from the **Date of Assessment** in the *Service Provider Definition Tab*. In the *Service Provider Definition Tab*, the **Date of Assessment** is the date that an individual provider has last been assessed.
- Defined Service Providers ID #s:** choices by entity type (Self, Prime, Sub) available for inclusion in one or more decision alternatives; entered by user. (This menu is on the far right in the tab).

- ONSAT uses the ID#s generated for individual providers in the *Service Provider Definition* Tab to prepopulate the choices in the **Entity Type Column** (Self, Prime, or Sub).
- In the **Entity Type Column** of Self, there are three options: Self Past (ID #1), Self Now (ID #2), and Self Future (ID #3).
  - **Self Past** is handy as a benchmark reference, but is normally not a component for a decision alternative.
  - **Self Now** should remain in the provider list because assessing your own capability to provide the service based on trustworthiness of your business practices and maturity of your implemented security is a best practice.
  - **Self Future** represents that portion of the business that remains in-house. With the exception of Self Now, all decision alternatives should include Self Future.
- In the **Entity Type Column** of Prime, the three options in the example are Alpha Inc. (ID#4), Bravo Inc. (ID#5), and Charlie Inc. (ID#6).
- In the **Entity Type Column** of Sub, the three options in the example are Delta Inc. (ID#7), Echo Inc. (ID#8) and Foxtrot Inc. (ID#9)
- **Short Title:** used to create the **Decision Alternative Specific Label**; for every **Defined Service Provider ID #** entered, ONSAT populates the corresponding **Short Title** in the **Selected Provider by Entity Type** columns.
- **Decision Alternative Specific Label:** a unique identifier used for a decision alternative throughout the assessment process. When all the providers have been selected for a single decision alternative, ONSAT populates the **Decision Alternative Specific Label** by concatenating the **Short Titles** and the **Date of Assessment** as shown in the below example.

		Entity Type Column			Selected Provider By Entity Type				
		SELF	PRIME	SUB	SELF	PRIME	SUB		
	Choices=>	1,2,3	4,5,6	7,8,9				Decision Alternative Specific Label (Defined Here)	
Date of Assessment	User Defined Specific Label								
12/18/2019		3	6		Self Future	Charlie Inc.		Decision Alt.	Self Future / Charlie Inc. / _ - 12/18/2019
12/18/2019	ABC Inc.	3	6		Self Future	Charlie Inc.		Decision Alt.	ABC Inc. _ ] - 12/18/2019

- The ONSAT-generated **Decision Alternative Specific Label** is the default; however, a **User Defined Alternative Specific Label** field is available.
  - If the **User Defined Specific Label** field is blank, then ONSAT generates the **Decision Alternative Specific Label** as described above.
  - If the **User Defined Specific Label** field is populated, then ONSAT generates the **Decision Alternative Specific Label** by concatenating the **User Defined Specific Label** and the **Date of Assessment**.

Using the template in the *Decision Alternative Definition* Tab, enter the following information (also see Figure 26, next page):

- Enter the **Date of Assessment**:

- The **Date of Assessment** for the *Decision Alternative Definition* Tab can be the same as the **Date of Assessment** in the *Service Provider Definition* Tab.
  - It is more likely that the **Date of Assessment** in the *Service Provider Definition* Tab will vary between providers for multiple reasons; for example, company policy may dictate that existing providers be reevaluated prior to consideration in an outsourcing decision.
- The **Date of Assessments** are likely to occur in shorter intervals in the *Decision Alternative Definition* Tab to coincide with the allotted time for the outsourcing decision.

		Entity Type Column			Selected Provider By Entity Type			
		SELF	PRIME	SUB	SELF	PRIME	SUB	Defined Service Providers
	Choices=>	1,2,3	4,5,6	7,8,9				
Date of Assessment	User Defined Specific Label				Decision Alternative Specific Label (Defined Here)			
								1 Self Past
								2 Self Now
								3 Self Future
								4 Alpha Inc.
								5 Bravo Inc.
								6 Charlie Inc.
								7 Delta Inc.
								8 Echo Inc.
								9 Foxtrot Inc.

Figure 26: Decision Alternative Definition Starting Point

- Input the **Defined Service Providers ID #** of the chosen provider in each **Entity Type Column** to create a decision alternative. Repeat the process until all decision alternatives are entered in the template. Note: The entity type of a provider can be modified from project to project or based on specific requirements.
  - Only **one** provider from each **Entity Type Column** can be selected to build a decision alternative.
    - Self Now (ID #2) stands by itself as a decision alternative and represents the option of **not** outsourcing the service.
    - Self Future (ID #3) requires a provider(s) to be chosen from the Prime **Entity Type Column**, the Sub **Entity Type Column**, or both the Prime and Sub **Entity Type Columns**.
  - The entity type of each provider must be used as defined in the *Service Provider Definition* Tab with one exception.
    - Exception: ONSAT allows the user to select a sub provider to function as a prime without modifying the entity type. For example, in the decision alternatives below, a prime provider is not selected but a sub provider is selected. Thus, the sub provider is functioning as the prime.

		Entity Type Column			Selected Provider By Entity Type				
		SELF	PRIME	SUB	SELF	PRIME	SUB		
	Choices=>	1,2,3	4,5,6	7,8,9				Sub as a Prime	Decision Alternative Specific Label (Defined Here)
Date of Assessment	User Defined Specific Label								
12/18/2019		3		7	Self Future		Delta Inc.	Decision Alt. [ Self Future / _ / Delta Inc. ] - 12/18/2019	
12/18/2019		3		8	Self Future		Echo Inc.	Decision Alt. [ Self Future / _ / Echo Inc. ] - 12/18/2019	

### 3.2 Step 2: Collect and Appraise Evidence

The Assessment Process encourages an evidence-based approach and step two in the process calls for collecting and appraising evidence. Note that there are not corresponding tabs in the tool for collecting and appraising evidence. The reasons for not having an evidence tab in the tool are two-fold: 1) the tool does not have the functionality to database large amounts of data, including potentially sensitive business information supplied by potential outsourcing partners, and 2) sources of evidence will most likely differ depending on the user, business case, or industry type.



It is often the case in the contracting environment for the outsourcing organization to assess the prime, and hold the prime accountable for its subcontractors' performance. As such, the prime should leverage ONSAT to assess its sub(s) and include evidence of the sub's Business Trust and Security Maturity when supplying information for review by the outsourcing organization. It is also a viable option for the sub to provide responses to the assessments, and associated evidence, directly to the outsourcing organization depending on contract restrictions and business agreements. Although tabs within the tool for collecting and appraising evidence are not present, this step in the process is critical as it links directly to substantiating the trustworthiness and security maturity level of an existing or potential partner. Collecting and appraising evidence is highly subjective and requires some ad hoc review of self and partner information; this approach is encouraged to facilitate the tool effectiveness.

#### 3.2.1 Defining Evidence

In the context of this tool, the starting point for evidence-based management is that management decisions rely on a combination of critical thinking and the best available evidence. The term "evidence" refers to information, facts or data supporting (or contradicting) a claim, assumption or hypothesis. Evidence may come from scientific research, but internal business information and even professional experience can count as "evidence".<sup>22</sup> In the context of this user manual and tool, evidence can be any source of information the assessor or the assessor's organization *deems credible, transferable, dependable, and confirmable*. Together these characteristics form the basis of trustworthiness as part of qualitative research<sup>23</sup>.

- **Credibility:** the confidence in the "veracity" of the findings i.e. "How do you know that your findings are true and accurate?"<sup>24</sup>

<sup>22</sup> Barends, E., Rousseau, D.M., & Briner, R.B. (2014). *Evidence Based Management: The Basic Principles*. Amsterdam: Center for Evidence-based Management

<sup>23</sup> Statistics Solutions. (2016, December 19). What is Trustworthiness in Qualitative Research? [Blog post]. Retrieved from <http://www.statisticssolutions.com/what-is-trustworthiness-in-qualitative-research/>

<sup>24</sup> Statistics Solutions. (n.d.). What is credibility in qualitative research and how do we establish it? [Blog post]. Retrieved from <https://www.statisticssolutions.com/what-is-credibility-in-qualitative-research-and-how-do-we-establish-it/>



- **Transferability:** the findings are applicable to other contexts e.g. similar situations / endeavors, and/or similar populations<sup>25</sup>
- **Dependability:** the reliability of the assessment i.e., similar findings would be obtained if assessment repeated<sup>26</sup>
- **Confirmability:** the objectivity of the assessor and/or researcher i.e., the findings of a study are shaped by the respondents and not researcher bias, motivation, or interest<sup>27</sup>

### 3.2.2 Sources and Examples of Evidence

Sources of evidence will vary based on the size and type of the organization as well as the existing maturity level of the organization's security and business processes in effect. Similarly, the format of evidence will vary. Examples of evidence sources include:

- Certifications and/or assessments against one of the **ten** Security Frameworks or Guidance currently mapped to the assessment tool;
- Vendor-supplied responses to questionnaires;
- Interviews, direct or second party documented previous experience with potential partners;
- Expert opinion;
- Formal documents submitted as part of a contract bidding process (DD Form 1155 Order for Supplies or Services or DD Form 254 Department of Defense Contract Security Classification Specification, both available for download at <https://www.esd.whs.mil/Directives/forms/>);
- Other formal documentation provided directly from provider or inspection organization:
  - Service Organization Control (SOC) reports: SOC1, SOC2, SOC3<sup>28</sup>;
  - Command Cyber Operational Readiness Inspection (CCORI)<sup>29</sup>;
  - Command Cyber Readiness Inspection (CCRI)<sup>30</sup>;
  - Security Inspection reports, and formal Security Self-Inspection reports/letters;
- Contractor Performance Assessment Reporting System (CPARS)<sup>31</sup>;
- Commercial "Intelligence" Sources:
  - LexisNexis<sup>32</sup>;
  - Dun & Bradstreet<sup>33</sup>;
  - Factiva<sup>34</sup>;
- Other e.g. Google

---

<sup>25</sup> Lincoln, YS. & Guba, EG. (1985). [Naturalistic Inquiry](http://www.qualres.org/HomeLinc-3684.html). Newbury Park, CA: Sage Publications. Retrieved from <http://www.qualres.org/HomeLinc-3684.html>

<sup>26</sup> ibid

<sup>27</sup> ibid

<sup>28</sup> <https://www.cm-alliance.com/news/2016/05/us-client-want-isaec-soc-2-report-i-already-iso-27001-certified-i>

<sup>29</sup> <https://www.afcea.org/content/new-perspective-aids-cyber-inspections-amid-mission-risk>

<sup>30</sup> <https://securestrux.com/core-capabilities/ccri/>

<sup>31</sup> <https://www.cpars.gov/>

<sup>32</sup> Get critical intelligence with help from Lexis Diligence. (2015). Retrieved from <https://www.lexisnexis.com/pdf/Lexis-Diligence/lexis-diligence-overview.pdf>

<sup>33</sup> Our Supply Chain Management Products. Retrieved from <https://www.dnb.com/products/operations-supply.html>

<sup>34</sup> <https://professional.dowjones.com/factiva/>



### 3.2.3 Appraising Evidence

According to Barends, Rousseau, and Briner (2014), “Evidence-based practice is about making decisions through the conscientious, explicit and judicious use of the best available evidence from multiple sources” (p.4). Therefore, it is a good practice to appraise evidence, by judging the trustworthiness and relevance of the evidence.<sup>35</sup> Once appraised, it is helpful to create a hierarchy of evidence as a visual reference (Figure 27). Additionally, internal processes can call for combinations of evidence types e.g. review by an expert should always accompany other evidence used.

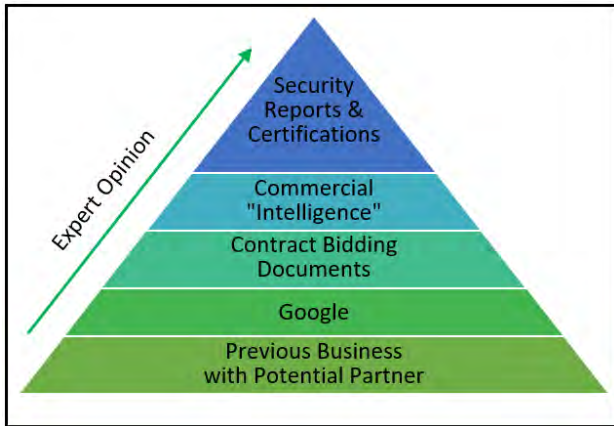
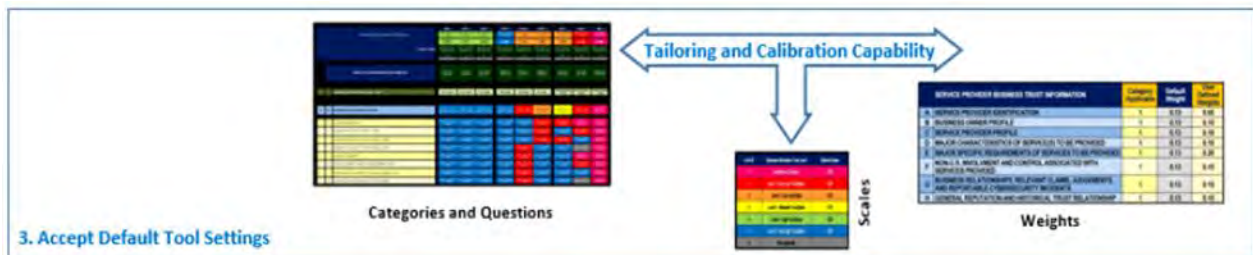


Figure 27: Sample Evidence Hierarchy

### 3.3 Step 3: Accept Default Tool Settings

Tool settings are prepopulated in ONSAT and can be reviewed in the Default Tool Settings Tab. By accepting the default settings, ONSAT is able to capture and aggregate overall comparison scores from the three intertwined assessments. To enable comparison, ONSAT uses a Weighted Average as the Basic Aggregation Function for Questions, Categories, and Decision Criteria.



ONSAT can be tailored based on the type of industry, size of organization or specific needs of the services being outsourced. For example, the percentage of importance of each of the assessments to the outsourcing decision can be reflected by weighting one assessment heavier. Similarly, individual categories and/or questions can be weighted heavier in either the business trust assessment or security maturity assessment. One reason for raising the weights of specific security categories might be an organization’s intent to offset an area of less mature security practices. Note: The tabs used to change the default settings are listed in Annex 4: Tool Settings Adjustment. However, this user manual provides instructions based on the default tool setting as described in the table below (Figure 28).

<sup>35</sup> Barends, E., Rousseau, D.M., & Briner, R.B. (2014). *Evidence Based Management: The Basic Principles*. Amsterdam: Center for Evidence-based Management. <https://www.cebma.org/wp-content/uploads/Evidence-Based-Practice-The-Basic-Principles.pdf>

Tab Name	Description	Default Setting
Decision Criteria-Weight Definition	Percentage of Importance of each of the Assessments (Business, Security, Financial) to the Outsourcing Decision	All three assessments equally weighted
Scale Format Definition	Defines the scales used in the analysis of the decision alternatives as listed below. Information Verification Levels Information Trust Basis Levels Security Maturity Levels	All scale definitions and values used as defined.
Business Category Definition	Defines the eight Business Categories comprising business trust	All eight categories used as defined.
Business Questions Definition	Defines the Business Trust Questions used in the Analysis of Decision Alternatives	All 75 questions used as defined
Business Category Weights	Defines the Weights of each Category of Business Trust Used in the Analysis of Decision Alternatives	Categories equally weighted
Business Question Weights	Defines the Weights of Business Trust Questions within each Category Used in the Analysis of Decision Alternatives	Questions within a category equally weighted
Security Category Definition	Defines the Security Categories Used in The Analysis of Decision Alternatives	All eighteen categories used as defined.
Security Questions Definition	Defines the Security Questions Used in the Analysis of Decision Alternatives	All 90 questions used as defined
Security Category Weights	Defines the Weights of the Categories of Security Used in the Analysis of Decision Alternatives	Categories equally weighted
Security Question Weights	Defines the Weights of the Security Questions within a Category Used in the Analysis of Decision Alternatives	Questions within a category equally weighted

Figure 28: Default Tool Settings

The individual scales used for the Business Trust and Security Maturity Assessments are detailed in Section 2.1.3 Business Trust and Security Maturity Assessments and Associated Scales. For easy reference, all default assessment scales are depicted side-by-side in the table below (Figure 29).

Business Information Verification Scale			Business Information Trust Basis Scale			Security Maturity Scale		
Level ID	Business Information Verification Level	Defined Values	Level ID	Business Information Trust Level	Defined Values	Level ID	Security Maturity Level	Defined Values
0	Insufficient Evidence	0.00	0	Insufficient Evidence	0.00	0	Insufficient Evidence	0.00
1	Level 1 - Unverified Information	0.20	1	Level 1 - Very Low Trust Basis	0.20	1	Level 1 - Undefined, Undocumented	0.20
5	Level 5 - Verified Information	0.95	2	Level 2 - Low Trust Basis	0.50	2	Level 2 - Defined, Limited Scope	0.50
6	Not Applicable		3	Level 3 - Moderate Trust Basis	0.75	3	Level 3 - Corporate Standard	0.75
			4	Level 4 - High Trust Basis	0.85	4	Level 4 - Quantitatively Managed	0.85
			5	Level 5 - Very High Trust Basis	0.95	5	Level 5 - Corporate Optimization	0.95
			6	Not Applicable		6	Not Applicable	

Figure 29: Business Trust and Security Maturity Assessment Scales

## 4.0 Step 4: Assess Providers Using Evidence



### 4.1 Identify the Individual or Team Conducting the Assessment

Successful risk management when outsourcing network services is dependent upon the alignment between the maturity of security and business practices in place. Therefore, it is important to ensure representation from pertinent departments across the organization or business that have the authority

to inform the assessment and ultimately the business decision. The assessments are subjective evaluations based on the best available evidence.

Assessors can be a group of individuals, a formal or informal panel, ad-hoc assembled set of experts, or a single individual. Whether an individual or a team approach is used, it is critical to assemble the knowledge and experience to vet the decision alternatives. Typically, the assessment is a team approach that involves personnel representing all aspects of the business. Critical team representation starts with the Chief Technology Officer's (CTO) organization. Enterprise Technology, Data Compute and Shared Services personnel add insight into the assessment from an operational perspective. Of particular importance, the Chief Information Security Officer and Data Protection Officer teams need to be involved to ensure cyber security and data assurance protocols are addressed. A senior member of the Governance, Risk & Compliance team is critical to adequately assess the overall risk impact to the corporate information system environment. Outside of the CTO organization, it is important to have Human Resources, Legal, Finance and Procurement representatives to ensure standard corporate policy and procedures are reviewed when they are applied to any outside services acquisition. It is important to proactively identify and leverage guidance on "acceptable" Financial Cost, and the minimum required levels of Business Trust and Security Maturity. Continuous interaction among departments is a best practice identified in early pilots of the tool. This user manual will follow the typical team approach.

#### 4.2 Define the Internal Process

The assessment process should leverage the CTO's organizational program for standard IT Environment Change Management. Similar to any other Information Technology tool or process; the addition of ANY system(s) should undergo a review that addresses the introduction of any threat to confidentiality, integrity or availability to the corporate data processing infrastructure. A formalized Change Management program will typically insure that all relevant members of the IT organization provide a go/no-go review of proposed operating environment adjustments. The tool assists this Change Management review by highlighting risks and providing an informed decision to address those risks.

To ensure quality and consistency of each assessment using ONSAT, it is important to follow an internal process with established roles and responsibilities, guidance for scoring and arbitration, including evaluation of best available evidence. Capturing the assumptions, rationale behind scoring, raised concerns, and clarifications for later reference should be part of the internal process. Group decision facilitation, "Wisdom of Crowds" techniques, and sensitivity analysis can help support team-approach assessments.

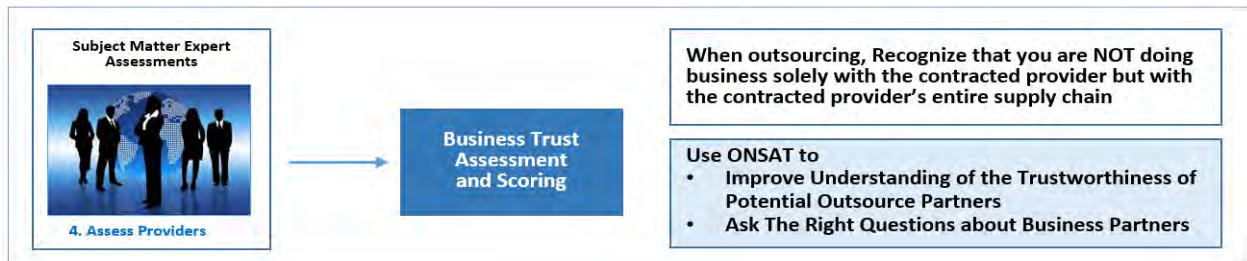
Examples of scoring arbitration approaches:

- **Consensus:** everyone must agree.
- **General Agreement:** captures the general inclination of the team.
- **Final Decision Authority:** makes final call based on team input.
- **Max OR Min:** use the max estimate or use the min estimate.
- **Average:** collect scores for each question across the team and use the integer nearest the average.
- **Detailed Average:** collect scores for each subcomponent focus of the question and use the integer nearest the average; then sum the averages of the subcomponents and use the integer nearest the average as the final score.

- For example, for the question below, the four subcomponents are **bolded** and effectively become four questions: *Are System Security, Personnel Security, Physical Security and Supply Chain Security Roles and Responsibilities **Defined, Documented, Assigned, and Implemented?***

Subcomponent Questions	Subcomponent Average
Are System Security, Personnel Security, Physical Security and Supply Chain Security Roles and Responsibilities <b>Defined</b> ?	4.0
Are they <b>Documented</b> ?	4.0
Are they <b>Assigned</b> ?	3.0
Are they <b>implemented</b> ?	2.0
Total	13
Average of Total	3.25
Integer nearest Average	3.0

### 4.3 Conduct a Business Trust Assessment



The Business Trust Assessment measures the level of business trust based on verification of facts about the organization combined with an evaluation of the organization’s abilities to meet all requirements of the outsourcing agreement. The first 30 questions are verification questions that assess factual business information using the Business Information Verification Scale.

Individual providers included in the *Decision Alternative Definition* Tab appear in vertical columns in the *Example Business Assessment* Tab (Figure 30, next page). The team of Subject Matter Experts, using the best available evidence, assesses each individual provider identified in the *Service Provider Definition* Tab. Once all questions in a category are answered, the assessment score for that category is displayed as shown below. Similarly, once all the questions in the Business Trust Assessment are answered, the Overall Business Trust Score is displayed in the top row of the assessment template. The Business Trust Scores for the individual providers are incorporated in the Aggregated Decision Alternative Scores.

*This is Blank Space*



SERVICE PROVIDER BUSINESS INFORMATION			Self		Prime			Sub			
			Overall Business Trust Score	Level 4 - High Trust Basis	Level 4 - High Trust Basis	Level 5 - Very High Trust Basis	Level 2 - Low Trust Basis	Level 2 - Low Trust Basis	Level 2 - Low Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
			0.91	0.92	0.95	0.73	0.62	0.69	0.27	0.00	
Self Past (Not Evaluated)			Self Now 12/18/19	Self Future 12/18/19	Alpha Inc. 12/18/19	Bravo Inc. 12/18/19	Charlie Inc. 12/18/19	Delta Inc. 12/18/19	Echo Inc. 12/18/19	Foxtrot Inc. 12/18/19	
A	SERVICE PROVIDER IDENTIFICATION		Category Score	Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 1 - Unverified Information	Level 1 - Unverified Information	Level 1 - Unverified Information	Insufficient Information
V	1	Company/Business name		Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 1 - Unverified Information	Insufficient Information	Insufficient Information
V	2	Company Primary Service Provider Location		Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Insufficient Information
V	3	Company Primary Service Provider Business Contact		Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 1 - Unverified Information	Level 5 - Verified Information	Insufficient Information
V	4	Company Primary Service Provider Security Contact		Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 5 - Verified Information	Level 5 - Verified Information	Not Applicable	Insufficient Information
V	5	Company Headquarters		Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 5 - Verified Information	Level 5 - Verified Information	Insufficient Information	Insufficient Information
V	6	Company Regional Locations Associated with this Service		Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Insufficient Information
V	7	Company Major Production Sites Associated with this Service		Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Insufficient Information
V	8	Company /Business /Primary Service Provider Notes		Level 5 - Verified Information	Level 5 - Verified Information	Level 5 - Verified Information	Level 1 - Unverified Information	Level 5 - Verified Information	Level 5 - Verified Information	Not Applicable	Insufficient Information

Figure 30: Example Business Assessment Tab Part 1

The remaining 45 questions assess ability of the potential or existing provider to perform the needed services while satisfying legal, technical, and performance specifications. The Business Information Trust Basis scale is used to assess these questions. Notice in the example below Self Future has a higher trust basis score than Self Now for Category E, questions 50 and 51. The increased trust basis score is based on the assumption that with this function being outsourced to a partner capable of meeting the supply chain and subcontractor requirements and specifications, Self Future’s trust basis increases (Figure 31).

SERVICE PROVIDER BUSINESS INFORMATION			Self Past (Not Evaluated)	Self Now 12/18/19	Self Future 12/18/19	Alpha Inc. 12/18/19	Bravo Inc. 12/18/19	Charlie Inc. 12/18/19	Delta Inc. 12/18/19	Echo Inc. 12/18/19	Foxtrot Inc. 12/18/19
D	MAJOR CHARACTERISTICS OF SERVICE(S) TO BE PROVIDED			Level 3 - Moderate Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Insufficient Evidence	Insufficient Evidence
A	31	Assessment of Experience in Providing Network Services to Be Considered in this Assessment		Level 3 - Moderate Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
A	32	Assessment of Ability to Provide Support to Protect Major Business Functions Affected if Service is Not Provided as Specified		Level 3 - Moderate Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
A	33	Assessment of Ability to Protect Identified Sensitive Data Associated with this Service		Level 4 - High Trust Basis	Level 4 - High Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
A	34	Assessment of Ability to Satisfy Major Legal Requirements / Issues / Exposure Associated with this Service		Level 5 - Very High Trust Basis	Level 5 - Very High Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
A	35	Assessment of Ability to Implement Defined Service Provision		Level 4 - High Trust Basis	Level 4 - High Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 5 - Very High Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
E	MAJOR SPECIFIC REQUIREMENTS OF SERVICES TO BE PROVIDED			Level 4 - High Trust Basis	Level 4 - High Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 3 - Moderate Trust Basis	Insufficient Evidence	Insufficient Evidence
A	36	Assessment of Ability to Satisfy Major Service Level Agreement Performance Specification / Requirements		Level 5 - Very High Trust Basis	Level 5 - Very High Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 4 - High Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
A	50	Assessment of Ability to Satisfy Major Supply Chain Security and Delivery Specifications / Requirements	Increase in Self Future's Trust Basis	Level 2 - Low Trust Basis	Level 4 - High Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 4 - High Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
A	51	Assessment of Ability to Satisfy Major Subcontractor Provider Specification / Requirements		Level 3 - Moderate Trust Basis	Level 4 - High Trust Basis	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 4 - High Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence

Figure 31: Example Business Assessment Tab Part 2



All questions in the *Business Assessment* Tab are pre-loaded with “Insufficient Evidence” level values as the starting point (Figure 32). Self Past is useful as a reference especially in trend analysis, but it is normally not a component for an outsourcing decision alternative. The Self Past column is grayed out in the example. Using the template in the *Business Assessment* Tab, assess each of the providers.

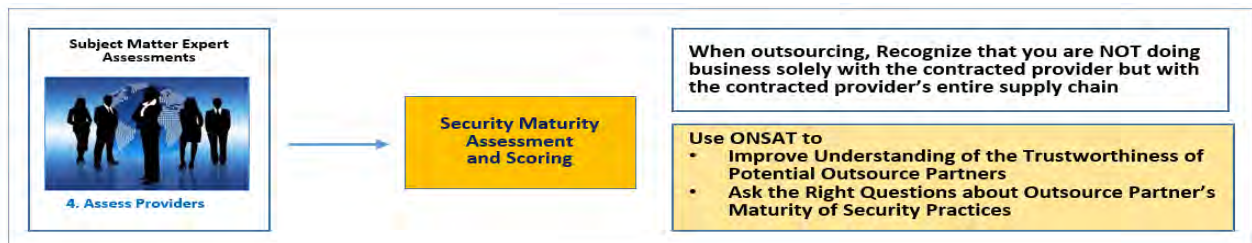
- Beginning in the Self Now column, evaluate evidence and assign a level from the drop-down menu for each question (Figure 32).
  - For categories A, B and C, the levels in the drop down menu are from the Business Information Verification Scale.
  - For categories D, E, F, G and H, the levels in the drop down menu are from the Business Information Trust Basis Scale.
- Repeat this step for each of the remaining providers.

A copy of the information entered in the *Business Trust Assessment* template is presented in the *Business Data Display* Tab. Analysis of the *Business Trust Assessment* results is covered in [Step 5: Examine Assessment Results and Analyze Decision Alternatives](#).

SERVICE PROVIDER BUSINESS INFORMATION			Self			Prime			Sub		
			Not Evaluated	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence
			Self Past Not Evaluated	Self Now 12/18/19	Self Future 12/18/19	Alpha Inc. 12/18/19	Bravo Inc. 12/18/19	Charlie Inc. 12/18/19	Delta Inc. 12/18/19	Echo Inc. 12/18/19	Foxtrot Inc. 12/18/19
		Input	Input	Input	Input	Input	Input	Input	Input		
A	SERVICE PROVIDER IDENTIFICATION		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	
V	1 Company/Business name		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	
V	2 Company Primary Service Provider Location		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	
V	3 Company Primary Service Provider Business Contact		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	
V	4 Company Primary Service Provider Security Contact		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	
V	5 Company Headquarters		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	
V	6 Company Regional Locations Associated with this Service		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	
V	7 Company Major Production Sites Associated with this Service		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	
V	8 Company /Business /Primary Service Provider Notes		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	

Figure 32: Business Assessment Tab Starting Point

#### 4.4 Conduct a Security Assessment



The Security Maturity Assessment measures the maturity of implemented security practices. Based on the available evidence, the assessor determines if, and how well, the security practice called out in each question is currently implemented and selects the most appropriate maturity level from the security scale.

Individual providers included in the *Decision Alternative Definition* Tab appear in vertical columns as shown in the *Example Security Assessment* Tab (Figure 33). The team of Subject Matter Experts, using the best available evidence, assesses each provider identified in the *Service Provider Definition* Tab. Once all questions in a category are answered, the category score is displayed. Similarly, once all the questions in the assessment are answered, the Overall Security Maturity Score is displayed. The Security Maturity Scores for the providers are incorporated in the Aggregated Decision Alternative Scores.

		Overall Security Maturity Score	Level 2 - Defined, Limited Scope	Level 2 - Defined, Limited Scope	Level 1 - Undefined, Undocumented	Level 1 - Undefined, Undocumented	Level 5 - Corporate Optimization	Level 1 - Undefined, Undocumented	Insufficient Evidence	Insufficient Evidence
Security Maturity Assessment		0.65	0.67	0.46	0.20	0.95	0.40	0.00	0.16	
		Self Now 12/18/19	Self Future 12/18/19	Alpha Inc. 12/18/19	Bravo Inc. 12/18/19	Charlie Inc. 12/18/19	Delta Inc. 12/18/19	Echo Inc. 12/18/19	Foxtrot Inc. 12/18/19	
1	RRR	1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]	Level 2 - Defined, Limited Scope	Level 3 - Corporate Standard	Level 1 - Undefined, Undocumented	Level 1 - Undefined, Undocumented	Level 5 - Corporate Optimization	Level 1 - Undefined, Undocumented	Insufficient Evidence	Insufficient Evidence
		Category Score								
1	RRR - 1.1	1) Are Critical Mission/Business Functions Defined and Documented and are Security Requirements and Business Practices Derived and Documented from those Functions?	Level 2 - Defined, Limited Scope	Level 3 - Corporate Standard	Level 4 - Quantitatively Managed	Level 1 - Undefined, Undocumented	Level 5 - Corporate Optimization	Level 2 - Defined, Limited Scope	Insufficient Evidence	Level 1 - Undefined, Undocumented
2	RRR - 1.2	2) Are System Security, Personnel Security, Physical Security and Supply Chain Security Roles and Responsibilities Defined, Documented, Assigned, and Implemented?	Level 2 - Defined, Limited Scope	Level 3 - Corporate Standard	Level 3 - Corporate Standard	Level 1 - Undefined, Undocumented	Level 5 - Corporate Optimization	Level 2 - Defined, Limited Scope	Insufficient Evidence	Level 1 - Undefined, Undocumented
3	RRR - 1.3	3) Are documented Security Requirements for Data Confidentiality, Integrity, and Availability, System Integrity and Availability, and Personnel/Process Integrity and Availability incorporated in both System Design and Business Practices?	Level 2 - Defined, Limited Scope	Level 4 - Quantitatively Managed	Level 2 - Defined, Limited Scope	Level 1 - Undefined, Undocumented	Level 5 - Corporate Optimization	Level 2 - Defined, Limited Scope	Insufficient Evidence	Level 1 - Undefined, Undocumented
4	RRR - 1.4	4) Does corporate management maintain oversight to ensure Mission/Business security requirements are in place as well as authorizing their implementation as well as holding responsible entities accountable?	Level 2 - Defined, Limited Scope	Level 5 - Corporate Optimization	Level 1 - Undefined, Undocumented	Level 1 - Undefined, Undocumented	Level 5 - Corporate Optimization	Level 2 - Defined, Limited Scope	Insufficient Evidence	Level 1 - Undefined, Undocumented
5	RRR - 1.5	5) Are Mission/Business security requirements incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?	Level 2 - Defined, Limited Scope	Level 4 - Quantitatively Managed	Insufficient Evidence	Level 1 - Undefined, Undocumented	Level 5 - Corporate Optimization	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence

Figure 33: Example Security Assessment Tab

All RRR questions in the *Security Assessment* Tab are pre-loaded with “Insufficient Evidence” level values as the starting point (Figure 34).

		Security Maturity Assessment Starting Point	Self Past 12/18/19	Self Now 12/18/19	Self Future 12/18/19	Alpha Inc. 12/18/19	Bravo Inc. 12/18/19	Charlie Inc. 12/18/19	Delta Inc. 12/18/19	Echo Inc. 12/18/19	Foxtrot Inc. 12/18/19
Cat # / ? ID	Ref ID	Category / Question	Not Evaluated	User Input	User Input	User Input	User Input	User Input	User Input	User Input	User Input
1	RRR	1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence
1	RRR - 1.1	1) Are Critical Mission/Business Functions Defined and Documented and are Security Requirements and Business Practices Derived and Documented from those Functions?		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence
2	RRR - 1.2	2) Are System Security, Personnel Security, Physical Security and Supply Chain Security Roles and Responsibilities Defined, Documented, Assigned, and Implemented?		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence
3	RRR - 1.3	3) Are documented Security Requirements for Data Confidentiality, Integrity, and Availability, System Integrity and Availability, and Personnel/Process Integrity and Availability incorporated in both System Design and Business Practices?		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence
4	RRR - 1.4	4) Does corporate management maintain oversight to ensure Mission/Business security requirements are in place as well as authorizing their implementation as well as holding responsible entities accountable?		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence
5	RRR - 1.5	5) Are Mission/Business security requirements incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?		Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence	Insufficient Evidence

Figure 34: Security Assessment Tab Starting Point

Using the template in the *Security Assessment* Tab, assess each of the providers starting in the Self Now column.

- For each question, evaluate evidence and assign a Security Maturity level using the drop-down menu.
- Based on analysis of available evidence, the assessment team determines if, and how well, the provider implements the security practice cited in the question.
  - Evaluation verbs are employed in each question to aid analysis of available evidence. Examples below demonstrate how to utilize evaluation verbs as cues to align with the level of security maturity (Figure 35).

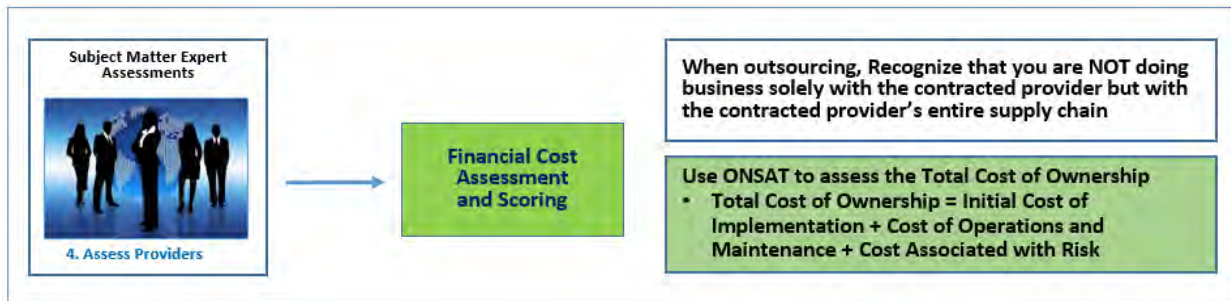
<b>16</b>	<b>GRC</b>	<b>16) Governance, Risk, and Compliance (GRC) Management Practices [System Governance]</b>
2	GRC - 16.2	2) Are Governance, Risk, and Compliance (GRC) Management Practices <b>implemented, coordinated, trained, and corporately managed</b> to meet Mission/Business Critical operations and obligations through routine and crisis situations?
Evaluation Cues →		If GRC Management Practices are <b>implemented and coordinated</b> but <b>not trained or corporately managed</b> , the assigned security maturity level should reflect this deficit.
<b>17</b>	<b>AIP</b>	<b>17) Asset HW/SW Integrity Protection Practices [Supply Chain]</b>
4	AIP - 17.4	4) Are Asset HW/SW incidents and violations <b>actively monitored, reported, documented, and effectively corrected</b> ?
Evaluation Cues →		If the incidents and violations are <b>actively monitored, reported, documented, and effectively corrected</b> , the assigned security maturity level should reflect a high level of implementation maturity.

Figure 35: Examples of Using Evaluation Verbs to aid assessment of evidence

- To address a known concern related to supply chain risk management when outsourcing network services, the fifth question in each category consistently uses the evaluation verbs of *incorporated* and *enforced* to assess how well security practices are incorporated into business practices and how well those business practices are enforced.
- Repeat this step for each of the remaining providers.

A copy of the information entered into the security assessment template is presented in the *Security Data Display* Tab. Analysis of the security assessment results is covered in [Step 5: Examine Assessment Results and Analyze Decision Alternatives](#).

#### 4.5 Conduct a Financial Assessment



The Financial Assessment uses the financial cost input for each provider in a decision alternative based on the role of the individual provider in the decision alternative. ONSAT assigns each decision alternative a cost utility value based on the entire service cost as a percentage of the maximum financial reference (maximum budget allotted). The utility values enable financial cost comparison of decision alternatives including the alternative to not outsource the service (Figure 36, next page).



			Decision Alternative Financial Cost Assessment													
							Cost Scenarios		Cost Components							
			Actual Data Being Used	Decision Alternatives	Self	Prime	Sub	All Contract Costs Included in Prime Cost (Self + Prime Cost)	All Contract Costs Included in Sub Cost (Self + Sub Cost)	Self Cost	Prime Cost	Sub Cost	Total Financial Cost	Financial Cost Level ID	Financial Cost Level	Financial Cost Utility Score
Overall Cost For Providers		\$ 18.0 (M)	User Defined Max Budget	Decision Alt. A - 12/18/2019	Self Now			Yes		\$ 17.5 (M)			\$ 17.5 (M)	1	Level 1 - Very High Cost Alternative	0.03
		\$ 18.0 (M)	Max Budget Used in Analysis	Decision Alt. B - 12/18/2019	Self Future	Alpha Inc.		Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Individual Provider Cost Input				Decision Alt. C - 12/18/2019	Self Future	Alpha Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
ID #	Providers	Financial Cost		Decision Alt. D - 12/18/2019	Self Future	Alpha Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
	(Entire Service Cost)			Decision Alt. E - 12/18/2019	Self Future	Alpha Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
1	Self Past 12/18/19	\$ 12.0 (M)		Decision Alt. F - 12/18/2019	Self Future	Bravo Inc.		Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
2	Self Now 12/18/19	\$ 17.5 (M)		Decision Alt. G - 12/18/2019	Self Future	Bravo Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
3	Self Future 12/18/19	\$ 6.0 (M)		Decision Alt. H - 12/18/2019	Self Future	Bravo Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
4	Alpha Inc. 12/18/19	\$ 4.0 (M)		Decision Alt. I - 12/18/2019	Self Future	Bravo Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
5	Bravo Inc. 12/18/19	\$ 6.0 (M)		Decision Alt. J - 12/18/2019	Self Future	Charlie Inc.		Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
6	Charlie Inc. 12/18/19	\$ 8.0 (M)		Decision Alt. K - 12/18/2019	Self Future	Charlie Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
7	Delta Inc. 12/18/19	\$ 5.5 (M)		Decision Alt. L - 12/18/2019	Self Future	Charlie Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
8	Echo Inc. 12/18/19	\$ 4.5 (M)		Decision Alt. M - 12/18/2019	Self Future	Charlie Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
9	Foxtrot Inc. 12/18/19			Decision Alt. N - 12/18/2019	Self Future		Delta Inc.	Yes		\$ 6.0 (M)	\$ 5.5 (M)	\$ 11.5 (M)	\$ 11.5 (M)	4	Level 4 - Low Cost Alternative	0.36
				Decision Alt. O - 12/18/2019	Self Future		Echo Inc.	Yes		\$ 6.0 (M)	\$ 4.5 (M)	\$ 10.5 (M)	\$ 10.5 (M)	5	Level 5 - Very Low Cost Alternative	0.42

Figure 36: Example Financial Assessment Tab

The *Financial Assessment* Tab can be described as an input side and a display side. The input side requires data entry in 3 areas: A, B, and C (Figure 36A). The outsourcing organization should be the source of information and evidence to complete all three sections. Field names are bolded.

Financial Cost Utility Assessment			Decision Alternatives				Cost Scenarios		
			Actual Data Being Used	Decision Alternatives	Self	Prime	Sub	All Contract Costs Included in Prime Cost (Self + Prime Cost)	All Contract Costs Included in Sub Cost (Self + Sub Cost)
<b>A</b>	Overall Cost For Providers	\$ 18.0 (M)	User Defined Maximum Budget	Decision Alt. A - 12/18/2019	Self Now			Yes	
		\$ 18.0 (M)	Maximum Budget Used in the Analysis	Decision Alt. B - 12/18/2019	Self Future	Alpha Inc.		Yes	
Individual Provider Cost Input				Decision Alt. C - 12/18/2019	Self Future	Alpha Inc.	Delta Inc.	Yes	
ID #	Providers	Financial Cost		Decision Alt. D - 12/18/2019	Self Future	Alpha Inc.	Echo Inc.	Yes	
	(Entire Service Cost)			Decision Alt. E - 12/18/2019	Self Future	Alpha Inc.	Foxtrot Inc.	Yes	
1	Self Past 12/18/19	\$ 12.0 (M)		Decision Alt. F - 12/18/2019	Self Future	Bravo Inc.		Yes	
2	Self Now 12/18/19	\$ 17.5 (M)		Decision Alt. G - 12/18/2019	Self Future	Bravo Inc.	Delta Inc.	Yes	
3	Self Future 12/18/19	\$ 6.0 (M)		Decision Alt. H - 12/18/2019	Self Future	Bravo Inc.	Echo Inc.	Yes	
4	Alpha Inc. 12/18/19	\$ 4.0 (M)		Decision Alt. I - 12/18/2019	Self Future	Bravo Inc.	Foxtrot Inc.	Yes	
5	Bravo Inc. 12/18/19	\$ 6.0 (M)		Decision Alt. J - 12/18/2019	Self Future	Charlie Inc.		Yes	
6	Charlie Inc. 12/18/19	\$ 8.0 (M)		Decision Alt. K - 12/18/2019	Self Future	Charlie Inc.	Delta Inc.	Yes	
7	Delta Inc. 12/18/19	\$ 5.5 (M)		Decision Alt. L - 12/18/2019	Self Future	Charlie Inc.	Echo Inc.	Yes	
8	Echo Inc. 12/18/19	\$ 4.5 (M)		Decision Alt. M - 12/18/2019	Self Future	Charlie Inc.	Foxtrot Inc.	Yes	
9	Foxtrot Inc. 12/18/19			Decision Alt. N - 12/18/2019	Self Future		Delta Inc.		Yes
				Decision Alt. O - 12/18/2019	Self Future		Echo Inc.		Yes

Figure 36A: Example Financial Assessment Tab: Input

- **Section A - Overall Cost for Providers** is the **User-defined Maximum Budget** for the provider(s) to deliver the service and can also serve as a cost figure for modeling and trend analysis.
  - The dollar amount entered populates the **Maximum Budget Used in Analysis** field needed to calculate the dollar amounts that align with the Cost Utility Scale Levels.

		Actual Data Being Used	
A	Overall Cost For Providers	\$ 18.0 (M)	User Defined Maximum Budget
		\$ 18.0 (M)	Maximum Budget Used in the Analysis

- Any cost amount *greater than \$0.00* is accepted. In the example, the **User-Defined Maximum Budget** is \$18.0 Million.
- If a **User-Defined Maximum Budget** entered is less than or equal to \$ 0.00, or if the field is left blank, then the **User-Defined Maximum Budget** is treated as if the value entered is zero and the Financial Display will show an error i.e. a **Cost Level ID** of 0 combined with **Cost Level** of “Over Budget” (below).

Error Message			
Total Financial Cost	Financial Cost Level ID	Financial Cost Level	Financial Cost Utility Score
\$ .0 (M)	0	Over Budget	0.00

- **Section B - Individual Provider Cost** is the entire service cost *per provider* as a component of a decision alternative.
  - Columns one (**ID #**) and two (**Short Title**) in this section are prepopulated from the providers listed in the *Decision Alternative Definition* Tab.
  - Service cost amounts are entered only for **Self and Prime Entity Types**.
  - In the example:
    - Self Now’s service cost represents the current cost to perform the function.
    - Self Future’s service cost represents the portion of the work that the outsourcing organization would still perform under an outsourcing arrangement.
    - Prime Providers’ (Alpha Inc., Bravo Inc. and Charlie Inc.) service costs represent the established practice of rolling up sub cost (and third-party vendors) into an aggregate cost presented to the outsourcing organization.
    - “Subs acting as a prime” represents a change in role / relationship between an outsourcing organization and a sub. Entering the service costs for Delta Inc. and Echo Inc. enables the decision alternatives to be vetted while complying with the entity type rule in ONSAT that a provider cannot represent more than one entity type in a decision alternative. In addition to being a Sub for each of the Prime’s, Delta Inc. and Echo Inc. are “subs acting as a prime”. Foxtrot Inc.’s



service cost is blank because in all alternatives, its service cost is reported under the Prime(s).

- **Section C – Cost Scenarios** are the aggregate cost descriptors that aid accuracy of the financial cost utility value.

- ONSAT’s **Cost Scenarios** are two mutually exclusive descriptors for aggregating cost amounts.
- Once service costs are entered for individual providers, a **cost scenario** is selected for each decision alternative.
- Only **one Cost Scenario** should be selected by toggling to “Yes” in the drop down menu.

Cost Scenarios	
All Contract Costs Included in Prime Cost (Self + Prime Cost)	All Contract Costs Included in Sub Cost (Self + Sub Cost)
Yes	
Yes	
Yes	
Yes	
	Yes
Yes	

- If *neither* **Cost Scenario** is toggled to “Yes”, the **Total Financial Cost** will display only the **Self Cost**, not the Sum Cost, and the Error Color of “Over Budget” will display.
- If *both* **Cost Scenarios** are toggled to “Yes”, the **Total Financial Cost** will display only the **Self Cost**, not the Sum Cost, and the Error Color of “Over Budget” will display.

Cost Scenarios		Cost Components			Total Financial Cost
All Contract Costs Included in the Prime Cost (Self + Prime Cost)	All Contract Costs Included in the Sub Cost (Self + Sub Cost)	Self Cost	Prime Cost	Sub Cost	
		\$ 6.0 (M)			\$ 6.0 (M)
Yes	Yes	\$ 6.0 (M)	\$ 4.0 (M)	\$ 5.5 (M)	\$ 6.0 (M)

- Decision Alternatives identified in the Decision Alternative Definition Tab are prepopulated in the columns to the left of the **Cost Scenario** as a reference.
  - In Decision Alternative A, Self Now, the first scenario is selected indicating that Self Now is reflecting all service cost or the **Total Financial Cost**.
  - For Alternatives (B, F and J), only Self Future and a prime are providers, the first scenario is selected.
  - For Alternatives (C, D, E, G, H, I, K, L, M), a sub is added but all contract costs are included in the **Prime Cost** (first scenario).
  - For Alternatives N and O, Delta Inc. and Echo Inc. are “subs acting as a prime”; thus, all contract costs are included in the **Sub Cost** (second scenario).

Decision Alternative Financial Cost Assessment				Cost Scenarios	
Decision Alternatives	Self	Prime	Sub	All Contract Costs Included in the Prime Cost (Self + Prime Cost)	All Contract Costs Included in the Sub Cost (Self + Sub Cost)
Decision Alt. A	Self Now			Yes	
Decision Alt. B	Self Future	Alpha Inc.		Yes	
Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.	Yes	
Decision Alt. D	Self Future	Alpha Inc.	Echo Inc.	Yes	
Decision Alt. E	Self Future	Alpha Inc.	Foxtrot Inc.	Yes	
Decision Alt. F	Self Future	Bravo Inc.		Yes	
Decision Alt. G	Self Future	Bravo Inc.	Delta Inc.	Yes	
Decision Alt. H	Self Future	Bravo Inc.	Echo Inc.	Yes	
Decision Alt. I	Self Future	Bravo Inc.	Foxtrot Inc.	Yes	
Decision Alt. J	Self Future	Charlie Inc.		Yes	
Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.	Yes	
Decision Alt. L	Self Future	Charlie Inc.	Echo Inc.	Yes	
Decision Alt. M	Self Future	Charlie Inc.	Foxtrot Inc.	Yes	
Decision Alt. N	Self Future		Delta Inc.		Yes
Decision Alt. O	Self Future		Echo Inc.		Yes

- Once a **Cost Scenario** is selected for each decision alternative, the input side of the Financial Assessment is completed.


For the display side, ONSAT calculates the **Financial Cost Utility Scale Level** information for each decision alternative using the **Maximum Budget Used in Analysis** value entered in the **Overall Cost for Providers** field in Section A.

- First, using the \$18 Million as the Maximum Budget, ONSAT calculates the dollar (\$) value for the **Lower Bound of Level** for each cost utility scale levels to align with the defined values e.g. 20% less than the Maximum Budget equates to \$14.4 Million (below).



Level ID	Financial Cost Utility Scale	Defined Values	Lower Bound of Level (\$ Value)
0	Over Budget	0.00	\$ 18.0 (M)
1	Level 1 - Very High Cost Alternative	0.10	\$ 16.2 (M)
2	Level 2 - High Cost Alternative	0.20	\$ 14.4 (M)
3	Level 3 - Moderate Cost Alternative	0.30	\$12.6 (M)
4	Level 4 - Low Cost Alternative	0.40	\$10.8 (M)
5	Level 5 - Very Low Cost Alternative	1.00	\$ .0 (M)
6	No Cost		

- Next, using the \$18 Million as the Maximum Budget, ONSAT calculates the **Financial Cost Utility Score** for each decision alternative using the below equation:
  - (Maximum Budget (\$) – Total Financial Cost) ÷ Maximum Budget (\$)
  - e.g. for Decision Alternative J: (\$18 M - \$14 M) ÷ (\$18 M) = 0.22



Decision Alternatives	Self	Prime	Total Financial Cost	Financial Cost Utility Score
Decision Alt. A	Self Now		\$ 17.5 (M)	0.03
Decision Alt. B	Self Future	Alpha Inc.	\$ 10.0 (M)	0.44
Decision Alt. F	Self Future	Bravo Inc.	\$ 12.0 (M)	0.33
Decision Alt. J	Self Future	Charlie Inc.	\$ 14.0 (M)	0.22

- Finally, ONSAT displays the **Total Financial Cost** and the associated **Financial Cost Utility Score** for each decision alternative on the display side of the *Financial Assessment* Tab (Figure 36B). The Financial Overall Assessment Scores (utility values) for the individual providers are incorporated in the aggregated scores of the decision alternatives. Analysis of the Financial Assessment results is covered in [Step 5: Examine Assessment Results and Analyze Decision Alternatives](#).

*This is Blank Space*

Decision Alternative Financial Cost Assessment										Financial Cost Utility		
Decision Alternatives	Self	Prime	Sub	Cost Scenarios		Cost Components			Total Financial Cost	Financial Cost Level ID	Financial Cost Level	Financial Cost Utility Score
				All Contract Costs Included in Prime Cost (Self + Prime Cost)	All Contract Costs Included in Sub Cost (Self + Sub Cost)	Self Cost	Prime Cost	Sub Cost				
Decision Alt. A - 12/18/2019	Self Now			Yes		\$ 17.5 (M)			\$ 17.5 (M)	1	Level 1 - Very High Cost Alternative	0.03
Decision Alt. B - 12/18/2019	Self Future	Alpha Inc.		Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Decision Alt. C - 12/18/2019	Self Future	Alpha Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Decision Alt. D - 12/18/2019	Self Future	Alpha Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Decision Alt. E - 12/18/2019	Self Future	Alpha Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Decision Alt. F - 12/18/2019	Self Future	Bravo Inc.		Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
Decision Alt. G - 12/18/2019	Self Future	Bravo Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
Decision Alt. H - 12/18/2019	Self Future	Bravo Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
Decision Alt. I - 12/18/2019	Self Future	Bravo Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
Decision Alt. J - 12/18/2019	Self Future	Charlie Inc.		Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
Decision Alt. K - 12/18/2019	Self Future	Charlie Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
Decision Alt. L - 12/18/2019	Self Future	Charlie Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
Decision Alt. M - 12/18/2019	Self Future	Charlie Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
Decision Alt. N - 12/18/2019	Self Future		Delta Inc.	Yes		\$ 6.0 (M)		\$ 5.5 (M)	\$ 11.5 (M)	4	Level 4 - Low Cost Alternative	0.36
Decision Alt. O - 12/18/2019	Self Future		Echo Inc.	Yes		\$ 6.0 (M)		\$ 4.5 (M)	\$ 10.5 (M)	5	Level 5 - Very Low Cost Alternative	0.42

Figure 36B: Example Financial Assessment Tab: Display

## 5.0 Step 5: Examine Assessment Results and Analyze Decision Alternatives

Security Scoring Summary					Decision Alternative ID																	
#	Provider	Security Score	Security Level	Security Level #	Rank	Alternative Participants			Total Value of Decision Alternative			Business Trust Assessment (Rating)			Security Implementation Assessment (Rating)			Financial Assessment (Rating)				
			Level 1 - Highest, Limited Scope	Level 2 - Medium, Limited Scope	Level 3 - Lowest, Limited Scope	Decision Alternative	Self	Primary	Sub	Rank (Order Change)	Overall Score	Overall Level	Overall Level ID	Business Trust Score	Business Trust Level	Business Trust Level ID	Security Implementation Score	Security Implementation Level ID	Security Implementation Level	Decision Alternative Cost (\$M)	Decision Alternative Cost (\$M)	Decision Alternative Cost (\$M)
2	Self Now 12/18/19	0.05	Level 1 - Highest, Limited Scope	2	3	Decision Alt. B - 10/23/2019	Self Now			1	0.02	Level 2 - Medium, Limited Scope	2	0.01	Level 4 - High Trust Basis	4	0.05	Level 2 - Medium, Limited Scope	2	0.20	\$ 15.0 (M)	1
4	Alpha Inc. 04/17/19	0.45	Level 1 - Highest, Limited Scope	1	5	Decision Alt. C - 10/22/2019	Self Now	Alpha Inc.		4	0.01	Level 2 - Medium, Limited Scope	2	0.01	Level 4 - High Trust Basis	4	0.05	Level 2 - Medium, Limited Scope	2	0.40	\$ 11.5 (M)	1
7	Delta Inc. 08/13/19	0.95	Level 3 - Lowest, Limited Scope	5	1	Decision Alt. D - 10/22/2019	Self Now	Alpha Inc.	Delta Inc.	7	0.02	Level 2 - Medium, Limited Scope	2	0.01	Level 4 - High Trust Basis	4	0.11	Level 2 - Medium, Limited Scope	2	0.40	\$ 11.5 (M)	1

### 5. Examine Assessment Results and Analyze Decision Alternatives

ONSAT’s approach uses the best available evidence to assess the Business Trust Level and the Security Maturity Level of individual providers as components of the decision alternatives. Similarly, ONSAT’s approach uses the best available evidence to assess the Financial Cost Utility Value of the decision



alternatives. The results of these three criteria assessments are a function of the quality of the evidence, experience and expertise of the assessor(s), and the definition of the weights, scales, and aggregation functions used. The incorporation of all three assessments into matrices for analysis of alternatives delivers informed decision making using a repeatable and scalable approach that can be tailored based on multiple factors including the type and size of organizations. To aid analysis, ONSAT provides visualization of Business Trust, Security Maturity, and Financial Cost Utility for individual providers as well as decision alternatives comprised of multiple providers. ONSAT supports drill-down analysis to the individual question level.

### 5.1 Individual Provider Results

ONSAT displays results of the individual providers to enable detailed review and comparative analysis. Analysis starts with examining the individual provider results by assessment type:

- **Business Trust:** Business Data Display, Provider Business Display, and Provider Business Category Display
- **Security Maturity:** Security Data Display, Provider Security Display, and Provider Security Category Display
- **Financial Cost:** Displays are at the summary and aggregated level

#### 5.1.1 Business Trust

The *Business Data Display* Tab is an exact copy of the data entered into the business assessment to serve as a reference, and as such is not displayed in the manual.

##### 5.1.1.1 Provider Business Display

The *Provider Business Display* Tab provides the Overall Business Trust Score and rank order for each provider assessed. Additionally, for each provider, the percentage of answers that fall within each **Business Trust Basis Level** is displayed (Figure 37).

Provider		Business Trust Assessment Score Summary				Distribution of Question Answers						
Provider ID	Provider	Overall Business Trust Score	Business Trust Basis Level	Business Trust Level ID	Rank Order	Blank	0.95	0.85	0.75	0.50	0.20	0.00
						Not Applicable	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 2 - Low Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence
2	Self Now	0.91	High Trust Basis	4	3	23%	68%	3%	5%	1%		
3	Self Future	0.92	High Trust Basis	4	2	23%	68%	5%	4%			
4	Alpha Inc.	0.95	Very High Trust Basis	5	1		100%					
5	Bravo Inc.	0.73	Low Trust Basis	2	4		17%	60%			23%	
6	Charlie Inc.	0.62	Low Trust Basis	2	6		24%		45%		16%	15%
7	Delta Inc.	0.69	Low Trust Basis	2	5	8%	29%	15%	17%	17%	8%	5%
8	Echo Inc.	0.27	Very Low Trust Basis	1	7	9%	11%				69%	11%
9	Foxtrot Inc.	0.00	Insufficient Evidence	0	8							100%

Figure 37: Example Provider Business Display Tab

Key information available from the display:

- Shows the range of Business Trust Scores across the providers.

- The top three performers for Business Trust are Alpha Inc. Self Future, and Self Now with little variance in their scores.
- Echo Inc. has a low trust score because 69% of its responses were Level 1.
- Highlights percentage range of scores across each of the eight categories.
  - Foxtrot Inc. has a low trust score because 100% of its responses did not provide sufficient evidence to-be assessed.

Review of the information in the *Provider Business Display* Tab prompts the need for additional analysis. For example, analysis tasks at this level:

- Using the *Provider Business Category Display* Tab to determine which category(s) of the Business Assessment is marked “Not Applicable” for Self Now, Delta Inc., and Echo Inc.
- Confirming that 100% of provided and/or available information for Foxtrot Inc. is insufficient evidence to assess Business Trust.

### 5.1.1.2 Provider Business Category Display

The *Provider Business Category Display* Tab duplicates the Overall Business Trust Score, the rank order, and distribution of question answers for each provider from the *Provider Business Display* Tab. New data to this display is the Business Trust Score for each provider across the eight Business Trust Categories. (Figure 38).

*Due to space limitations, the "Distribution of Question Answers" is not repeated below.*

Provider		Business Trust Assessment Scoring Summary				A - SERVICE PROVIDER IDENTIFICATION	B - BUSINESS OWNER PROFILE	C - SERVICE PROVIDER PROFILE	D - MAJOR CHARACTERISTICS OF SERVICE(S) TO BE PROVIDED	E - MAJOR SPECIFIC REQUIREMENTS OF SERVICES TO BE PROVIDED	F - NON-U.S. INVOLVEMENT AND CONTROL ASSOCIATED WITH SERVICES PROVIDED	G - BUSINESS RELATIONSHIPS, RELEVANT CLAIMS, JUDGEMENTS, AND REPORTABLE	H - GENERAL REPUTATION AND HISTORICAL TRUST RELATIONSHIP
Provider ID	Provider	Overall Business Trust Score	Business Trust Basis Level	Business Trust Level ID	Rank Order								
2	Self Now	0.91	High Trust Basis	4	3	0.95	0.95	0.95	0.83	0.91		0.95	0.85
3	Self Future	0.92	High Trust Basis	4	2	0.95	0.95	0.95	0.83	0.94		0.95	0.85
4	Alpha Inc.	0.95	Very High Trust Basis	5	1	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
5	Bravo Inc.	0.73	Low Trust Basis	2	4	0.48	0.49	0.62	0.85	0.85	0.85	0.85	0.85
6	Charlie Inc.	0.62	Low Trust Basis	2	6	0.67	0.66	0.62	0.75	0.75	0.00	0.75	0.75
7	Delta Inc.	0.69	Low Trust Basis	2	5	0.76	0.61	0.38	0.95	0.82	0.50	0.75	0.76
8	Echo Inc.	0.27	Very Low Trust Basis	1	7	0.38	0.35	0.46	0.20	0.20	0.20	0.20	0.20
9	Foxtrot Inc.	0.00	Insufficient Evidence	0	8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Figure 38: Provider Business Category Display Tab

Key information available from the display:

- Shows areas of strength and weakness for each provider across the Business Trust Categories.
  - Identifies the outsourcing organization’s lowest score as Category D.
  - Identifies providers with higher Business Trust Scores than Self Now in Category D.
- Displays score patterns across providers:
  - Bravo Inc.’s pattern of scores shows a low and very low trust score in the first three categories and a high trust score in the remaining five categories resulting in an Overall Business Trust Level that is two levels below Self Now.
  - Charlie Inc.’s score for Category F – Non-U.S. Involvement and Control Associated with Services Provided is 0.00 reflecting a rating of Insufficient Evidence.



- Delta Inc.’s score for Category D – Major Characteristics of Services to be Provided is at least two levels higher than its scores in any of the other categories; this information may prove useful in future displays depending on Delta Inc.’s role in an alternative.
- Echo Inc. has a Business Trust Score of Level 1 across all eight Business Trust Categories.
- Foxtrot Inc. has a Business Trust Score of Insufficient Evidence across all Categories.

Review of the information in the *Provider Business Category Display* Tab prompts the need for additional analysis. For example, analysis tasks at this level:

- Determining why Bravo Inc. scored lower in the Verification Section of the assessment, but scored consistently at a high level of Business Trust in the remainder of the assessment.
- Conferring with internal representatives e.g. legal, policy, procurement departments to ascertain the reason for Self Now’s “Not Applicable” response for all of Category F – Non-U.S. Involvement and Control Associated with Services Provided; refer to the Corporate Cloud Data Storage Services of U.S. Classified Information example in the *Outsourced Service Definition* Tab.
  - For example, an internal corporate policy or externally imposed constraint on services being performed / supplied by Non-U.S. Parties and Personnel could prompt the outsourcing organization to partner with a provider(s) that is not under the same restriction.
- Requesting evidence or improved evidence from Charlie Inc. for Category F; this is the single category in the Business Assessment for which Charlie Inc. has a score of Insufficient Evidence. Improving this category score could promote Charlie Inc. as a more viable candidate in Business Trust. **A Closer Look** at Charlie Inc.’s score in Category F is detailed in Section 5.4.5.

### 5.1.2 Security Maturity

The *Security Maturity Display* Tab is an exact copy of the data entered into the security assessment to serve as a reference, and as such is not displayed in the manual.

#### 5.1.2.1 Provider Security Display

The *Provider Security Display* Tab provides the Overall Security Maturity Score and rank order for each provider assessed. Additionally, for each provider, the percentage of answers that fall within each Security Maturity Level is displayed (Figure 39).

Security Maturity Assessment Scoring Summary				Distribution of Question Answers							
Provider ID	Provider	Overall Security Maturity Score	Rank Order	0.6	0.95	0.85	0.75	0.50	0.20	0.00	
				Not Applicable	Level 5 - Corporate Optimization	Level 4 - Quantitatively Managed	Level 3 - Corporate Standard	Level 2 - Defined, Limited Scope	Level 1 - Undefined, Undocumented	Insufficient Evidence	
1	Self Past 12/18/19			0%	18%	13%	26%	29%	9%	6%	
2	Self Now 12/18/19	0.65	3		11%	13%	32%	34%	9%		
3	Self Future 12/18/19	0.67	2		12%	16%	34%	29%	9%		
4	Alpha Inc. 12/18/19	0.46	4			20%	20%	20%	20%	20%	
5	Bravo Inc. 12/18/19	0.20	6						100%		
6	Charlie Inc. 12/18/19	0.95	1		100%						
7	Delta Inc. 12/18/19	0.40	5					80%		20%	
8	Echo Inc. 12/18/19	0.00	8							100%	
9	Foxtrot Inc. 12/18/19	0.16	7						80%	20%	

Figure 39: Example Provider Security Display Tab

Key information available from the display:

- Shows the range of Security Maturity Scores across the providers.
- Shows providers with a high level of Security Maturity.
  - The top performer for Security Maturity is Charlie Inc. Self Future, and Self Now have the next highest scores; but, their scores are three Security Maturity Levels lower.
- Shows the relationship between the Security Maturity Level and the Distribution of Answers for each provider; and highlights the informative value of evidence-based assessments.
  - For the highest scoring provider, Charlie Inc., 100% of the responses are in Level 5 Corporate Optimization indicating not only Charlie Inc.'s high Security Maturity Level, but also that the evidence available was at a “take it to the bank” credibility level.
  - For the lowest scoring provider, Echo Inc., 100% of the responses are in Level 0 Insufficient Evidence.

Review of the information in the *Provider Security Display* Tab prompts the need for additional analysis.

- Determining if the changes from initial trend analysis between Self Past and Self Now indicate increased attention to an evidence-based approach.

### 5.1.2.2 Provider Security Category Display

The *Provider Security Category Display* Tab duplicates the Overall Security Maturity Score, rank order, and the percentage of answers that fall within each Security Maturity Category from the *Provider Security Display* Tab. New data to this display is the Security Maturity Score for each provider across the eighteen Security Maturity Categories (Figure 40, next page).

*Due to space limitations, the "Distribution of Question Answers" is not repeated below.*

Security Maturity Assessment Scoring Summary						ONSAT Security Maturity Level Per Category																		
						Design Req. & Implement.		Data Flow	Asset & Audit	Information Assurance								Phys. Sec.	Per. Sec.	System Governance		Supply Chain		
						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
Provider ID	Provider	Overall Security Maturity Score	Security Maturity Level	Security Maturity Level ID	Rank Order	1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]	2) System Performance, Resiliency, and Security Architecture and Design Practices [System Design]	3) Communication Path, Data Flow, and Data Governance Policies and Practices [Data Governance]	4) Asset Inventory and Audit Management Practices [Asset & Audit]	5) Authentication and Access Control Practices [Info. Sys. Security]	6) Network Segmentation Practices [Info. Sys. Security]	7) Data Confidentiality, Integrity and Availability Protection Practices [Info. ]	8) Vulnerability and Resilience Management Practices [Info. ]	9) Configuration Management Practices [Info. ]	10) System Maintenance and Repairs Practices [Info. ]	11) Incident Detection and Response [Info. ]	12) Consequence / Impact Recovery Policies and Practices [Info. ]	13) Physical / Facilities Security Policies and Practices [Physical Security]	14) Personnel Security Policies, Awareness, and Training [Personnel Security]	15) Performance Management Practices [System Governance]	16) Governance, Risk, and Compliance (GRC) Management Practices [System Governance]	17) Asset HWSW Integrity Protection Practices [Supply Chain]	18) Supplier Documentation and Vetting Policy and Practices [Supply Chain]	
2	Self Now 12/18/19	0.65	Level 2 - Defined, Limited Scope	2	3	0.50	0.79	0.83	0.69	0.83	0.67	0.78	0.74	0.67	0.75	0.62	0.55	0.67	0.60	0.95	0.55	0.20	0.32	
3	Self Future 12/18/19	0.67	Level 2 - Defined, Limited Scope	2	2	0.83	0.79	0.83	0.69	0.83	0.67	0.78	0.74	0.67	0.75	0.62	0.55	0.67	0.60	0.95	0.55	0.20	0.32	
4	Alpha Inc. 12/18/19	0.46	Level 1 - Undefined, Undocumented	1	4	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46
5	Bravo Inc. 12/18/19	0.20	Level 1 - Undefined, Undocumented	1	6	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20
6	Charlie Inc. 12/18/19	0.95	Level 5 - Corporate Optimization	5	1	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
7	Delta Inc. 12/18/19	0.40	Level 1 - Undefined, Undocumented	1	5	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40
8	Echo Inc. 12/18/19	0.00	Insufficient Evidence	0	8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
9	Foxtrot Inc. 12/18/19	0.16	Insufficient Evidence	0	7	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16

Figure 40: Example Provider Security Category Display Tab

Key information available from the display:

- Shows areas of strength and weakness for each provider across the security maturity categories.
  - Identifies Charlie Inc.'s Security Maturity Scores as being at least two Security Maturity Levels higher than Self Now in seventeen categories and at the same level in the remaining category.
- Displays score patterns across providers:
  - The other two primes, Alpha Inc., and Bravo Inc., both have a Security Maturity of Level 1 Undefined, Undocumented across all eighteen categories.
  - For subs acting as a prime, Delta Inc., has a Security Maturity of Level 1 across all eighteen categories; and, Echo Inc. has a Security Maturity Level of Insufficient Evidence across all eighteen categories.
  - The remaining sub, Foxtrot Inc., has a Security Maturity Level of Insufficient Evidence across all eighteen categories.
- Shows an increase in score between Self Now (.50) and Self Future (.83) in Category 1: Mission and Security Requirements, Roles, Responsibilities and Policies [System Design].
  - The increase in Category 1 accounts for 100% of the overall difference in Security Maturity Scores between Self Now (.65) and Self Future (.67).

Review of the information in the *Provider Security Category Display* Tab prompts the need for additional analysis. For example:

- Determining the reason for the outsourcing organization's increased Category 1 score.
  - One explanation could be that by outsourcing, a portion of the roles and/or responsibilities to meet security requirements under System Design is also outsourced.
- Taking **A Closer Look** at Alpha Inc.'s Insufficient Evidence responses to determine if resolving them would significantly raise Alpha Inc.'s Overall Security Maturity Score. ONSAT's modeling capability is a good resource for this task (Figure41).

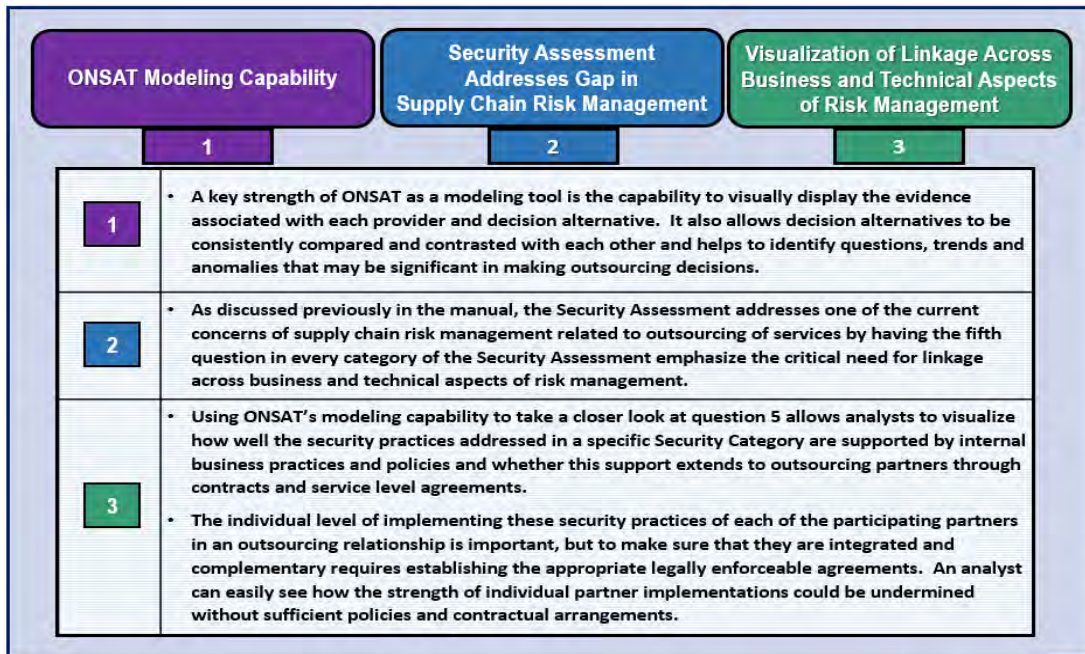


Figure 41: ONSAT's Modeling Capability Example



**A CLOSER LOOK... Potential Improvement in Alpha Inc.'s Security Maturity Score**

The *Provider Security Category Display* indicates that Alpha Inc. has a score of Level 1 Undefined, Undocumented for all Security Maturity Categories.

- This display also shows that 20 % of Alpha Inc.'s responses are rated as Insufficient Evidence with the remaining 80% of responses accounted for equally across Levels 1 – 4.

The *Example Security Assessment Tab* shows that the response pattern for Alpha Inc.'s Insufficient Evidence scores is Question 5 in all eighteen categories (see below). The *Example Security Assessment Tab* also reveals that Alpha Inc. has higher Security Maturity Scores for several questions in each category that are masked by the aggregated score at the category level.

Using the *Security Assessment Tab*:

- Modeling Alpha Inc.'s scoring for Question 5 in all Security Maturity Categories at Levels 2, 3, 4, and 5 does not significantly increase Alpha Inc.'s Overall Security Maturity Score. In fact, regardless of the Security Maturity Level value substituted for Insufficient Evidence, Alpha Inc.'s Overall Security Maturity Score does not increase above Level 2 Defined, Limited Scope.

Alpha Inc.	Current Category Security Maturity Level	Current Score
	Level 1 - Undefined, Undocumented	0.46
Question Number	Current Pattern for All 18 Categories Questions 1 – 4	Model Pattern for All 18 Categories Questions 1 – 4
1	Level 4 - Quantitatively Managed	Level 4 - Quantitatively Managed
2	Level 3 - Corporate Standard	Level 3 - Corporate Standard
3	Level 2 - Defined, Limited Scope	Level 2 - Defined, Limited Scope
4	Level 1 - Undefined, Undocumented	Level 1 - Undefined, Undocumented
	Current Pattern for All 18 Categories Question 5	Model Pattern for All 18 Categories Question 5
5	Insufficient Evidence	Level 1 - Undefined, Undocumented
	Insufficient Evidence	Level 2 - Defined, Limited Scope
	Insufficient Evidence	Level 3 - Corporate Standard
	Insufficient Evidence	Level 4 - Quantitatively Managed
	Insufficient Evidence	Level 5 - Corporate Optimization
		Model Overall Security Maturity Level and Score
		Level 2 - Defined, Limited Scope 0.50
		Level 2 - Defined, Limited Scope 0.56
		Level 2 - Defined, Limited Scope 0.61
		Level 2 - Defined, Limited Scope 0.63
		Level 2 - Defined, Limited Scope 0.63

This was a basic modeling exercise. Analyzing whether a change in the value for question 5 in each category would impact the scores in questions 1-4 is an example of more robust modeling.

## 5.2 Summary Views

Initial review of the assessment results is aided by a summary view of each of the three assessments. The *Business Summary Tab* and *Security Summary Tab* display a matrix with the individual providers on the vertical axis and associated scores on the horizontal axis. The *Financial Summary Tab* displays a matrix with the decision alternatives on the vertical axis and the associated scores on the horizontal axis.

### 5.2.1 Business Summary

For each provider in the *Business Summary Tab*, scores are displayed for each question, each Business Trust Category, and an Overall Business Trust Score also called the Aggregated Total Business Trust Score. The Aggregated Total Business Trust Scores feed the Aggregated Total Decision Alternative Scores referred to as an Aggregated Total Value Score in the tool (Figure 42).

Business Trust Assessment Comparison				ONSAT aggregates the Business Category Scores to determine an Aggregated Total Business Trust Score.								ONSAT aggregates the Individual Question Scores in a Category to determine a Business Trust Category Score.								
Aggregated Total Business Trust Score				Business Trust Category Name and Scores								Business Trust Category Name and Individual Question Scores								
Provider				Due to limited space, only Category D is shown.								D - Major Characteristics of Service(s) to be Provided								
ID #	Provider / Company Name	Aggregated Total Business Trust Score	Aggregated Total Business Trust Label	Aggregated Total Business Trust Level ID	A	B	C	D	E	F	G	H	1	2	3	4	5	6	7	8
					A – Service Provider Identification	B – Business Owner Profile	C – Service Provider Profile	D – Major Characteristics of Service(s) to be Provided	E – Major Requirements of Services to be Provided	F – Non-U.S. Involvement & Control Associated with Service(s) Provided	G – Business Relationships, Claims, Judgements, & Cybersecurity Incidents	H – General Reputation & Historical Trust Relationship	Company/Business name	Company Primary Service Provider Location	Company Primary Service Provider Business Contact	Company Primary Service Provider Security Contact	Company Headquarters	Company Regional Locations Associated with this Service	Company Major Production Sites Associated with this Service	Company /Business / Primary Service Provider Notes
2	Self Now	0.91	High Trust Basis	4	0.95	0.95	0.95	0.83	0.91		0.95	0.85	0.75	0.75	0.85	0.95	0.85	0.75	0.75	0.85
3	Self Future	0.92	High Trust Basis	4	0.95	0.95	0.95	0.83	0.94		0.95	0.85	0.75	0.75	0.85	0.95	0.85	0.75	0.75	0.85
4	Alpha Inc.	0.95	Very High Trust Basis	5	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
5	Bravo Inc.	0.73	Low Trust Basis	2	0.48	0.49	0.62	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85
6	Charlie Inc.	0.62	Low Trust Basis	2	0.67	0.66	0.62	0.75	0.75	0.00	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75
7	Delta Inc.	0.69	Low Trust Basis	2	0.76	0.61	0.38	0.95	0.82	0.50	0.75	0.76	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
8	Echo Inc.	0.27	Very Low Trust Basis	1	0.38	0.35	0.46	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20
9	Foxtrot Inc.	0.00	Insufficient Evidence	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Figure 42: Business Summary Tab

### 5.2.2 Security Summary

For each provider in the *Security Summary* Tab, scores are displayed for each question, each Security Maturity Category, each Functional Security Area, and an Aggregated Total Security Maturity Score also called the Overall Security Maturity Score (Figures 43A, next page and 43B, following page). The Aggregated Total Security Maturity Scores feed the Aggregated Total Value Scores of decision alternatives.

*This is Blank Space*



					ONSAT aggregates the Security Functional Area / Category Scores to determine an Aggregated Total Security Maturity Score.								
Security Maturity Assessment Comparison		Aggregated Total Security Maturity			Functional Security Area Scores								
ID #	Provider	Aggregated Total Security Maturity Score	Aggregated Total Security Maturity Level	Aggregated Total Security Maturity Level ID	A	B	C	D	E	F	G	H	
						A – Design Requirements & Implementation	B – Data Flow & Governance	C – Asset Inventory & Audits	D – Information Assurance	E – Physical Security	F – Personnel Security	G – System Governance	H – Supply Chain
2	Self Now	0.65	Defined, Limited Scope	2	0.65	0.83	0.69	0.70	0.67	0.60	0.75	0.26	
3	Self Future	0.67	Defined, Limited Scope	2	0.81	0.83	0.69	0.70	0.67	0.60	0.75	0.26	
4	Alpha Inc.	0.46	Undefined, Undocumented	1	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	
5	Bravo Inc.	0.20	Undefined, Undocumented	1	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	
6	Charlie Inc.	0.95	Corporate Optimization	5	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	
7	Delta Inc.	0.40	Undefined, Undocumented	1	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	
8	Echo Inc.	0.00	Insufficient Evidence	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	
9	Foxtrot Inc.	0.16	Insufficient Evidence	0	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	

Functional Security Areas		Security Maturity Category Scores																	
		A	B	C	D								E	F	G	H			
		1) Mission and Security Requirements, Roles, Responsibilities and Policies	2) System Performance, Resiliency, and Security Architecture and Design Practices	3) Communication Path, Data Flow, and Data Governance Policies and Practices	4) Asset Inventory and Audit Management Practices	5) Authentication and Access Control Practices	6) Network Segmentation Practices	7) Data Confidentiality, Integrity and Availability Protection Practices	8) Vulnerability and Resilience Management Practices	9) Configuration Management Practices	10) System Maintenance and Repairs Practices	11) Incident Detection and Response	12) Consequence / Impact Recovery Policies and Practices	13) Physical / Facilities Security Policies and Practices	14) Personnel Security Policies, Awareness, and Training	15) Performance Management Practices	16) Governance, Risk, and Compliance (GRC) Management Practices	17) Asset HW/SW Integrity Protection Practices	18) Supplier Documentation and Vetting Policy and Practices
Category #		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Self Now		0.50	0.79	0.83	0.69	0.83	0.67	0.78	0.74	0.67	0.75	0.62	0.55	0.67	0.60	0.95	0.55	0.20	0.32
Self Future		0.83	0.79	0.83	0.69	0.83	0.67	0.78	0.74	0.67	0.75	0.62	0.55	0.67	0.60	0.95	0.55	0.20	0.32
Alpha Inc.		0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46
Bravo Inc.		0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20
Charlie Inc.		0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
Delta Inc.		0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40	0.40
Echo Inc.		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Foxtrot Inc.		0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16

Figure 43A: Security Summary Tab

ONSAT aggregates the Individual Question Scores in a category to determine a Security Maturity Category Score.						
Functional Security Area	C – Asset Inventory and Audits					
Category	4) Asset Inventory and Audit Management Practices					
Question #	16	17	18	19	20	
	1) Are Mission/Business Critical operational assets inventoried and periodically audited to assure their initial and continued pedigree, accountability and integrity?	2) Are Mission/Business Critical backup, reserve, and replacement assets inventoried, and periodically audited to assure their initial and continued pedigree, accountability and integrity?	3) Are Asset Inventory and Audit data protected from loss, corruption, or manipulation and are asset inventory and audit data available for use and incorporated into defining the integrity of the Mission/Business critical functions and processes?	4) Are Asset Inventory and Audit data reviewed and assessed to support an effective known configuration of the system and processes and effective and timely corrective actions?	5) Are Asset Inventory and Audit Management Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?	
ID #	Provider					
2	Self Now	0.85	0.50	0.85	0.50	0.75
3	Self Future	0.85	0.50	0.85	0.50	0.75
4	Alpha Inc.	0.85	0.75	0.50	0.20	0.00
5	Bravo Inc.	0.20	0.20	0.20	0.20	0.20
6	Charlie Inc.	0.95	0.95	0.95	0.95	0.95
7	Delta Inc.	0.50	0.50	0.50	0.50	0.00
8	Echo Inc.	0.00	0.00	0.00	0.00	0.00
9	Foxtrot Inc.	0.20	0.20	0.20	0.20	0.00

Figure 43B: Security Summary Tab

### 5.2.3 Financial Summary

In the *Financial Summary* Tab, the Financial Cost Utility Score and the Total Financial Cost are displayed for each decision alternative. The providers of each alternative are listed as are the corresponding cost components. The Aggregated Total Financial Cost Utility Scores feed the Aggregated Total Value Scores.

*Due to space limitations, the cost input columns are not displayed.*

Decision Alternative Financial Cost Assessment				Cost Scenarios		Cost Components			Financial Cost			
Decision Alternatives	Self	Prime	Sub	All Contract Costs Included in Prime Cost (Self + Prime Cost)	All Contract Costs Included in Sub Cost (Self + Sub Cost)	Self Cost	Prime Cost	Sub Cost	Total Financial Cost	Financial Cost Level ID	Financial Cost Level	Financial Cost Utility Score
Decision Alt. A	Self Now			Yes		\$ 17.5 (M)			\$ 17.5 (M)	1	Level 1 - Very High Cost Alternative	0.03
Decision Alt. B	Self Future	Alpha Inc.		Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Decision Alt. D	Self Future	Alpha Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Decision Alt. E	Self Future	Alpha Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 4.0 (M)		\$ 10.0 (M)	5	Level 5 - Very Low Cost Alternative	0.44
Decision Alt. F	Self Future	Bravo Inc.		Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
Decision Alt. G	Self Future	Bravo Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
Decision Alt. H	Self Future	Bravo Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
Decision Alt. I	Self Future	Bravo Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 6.0 (M)		\$ 12.0 (M)	4	Level 4 - Low Cost Alternative	0.33
Decision Alt. J	Self Future	Charlie Inc.		Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
Decision Alt. L	Self Future	Charlie Inc.	Echo Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
Decision Alt. M	Self Future	Charlie Inc.	Foxtrot Inc.	Yes		\$ 6.0 (M)	\$ 8.0 (M)		\$ 14.0 (M)	3	Level 3 - Moderate Cost Alternative	0.22
Decision Alt. N	Self Future		Delta Inc.	Yes		\$ 6.0 (M)		\$ 5.5 (M)	\$ 11.5 (M)	4	Level 4 - Low Cost Alternative	0.36
Decision Alt. O	Self Future		Echo Inc.	Yes		\$ 6.0 (M)		\$ 4.5 (M)	\$ 10.5 (M)	5	Level 5 - Very Low Cost Alternative	0.42

Figure 44: Financial Summary

### 5.3 Aggregated Results and Integrated Decision Alternative Displays

ONSAT’s aggregated scoring and integrated alternative displays facilitate “rack and stack” analysis of the decision alternatives and “assists in translating available evidence into outsourcing decision-support information”, a key objective of ONSAT.

#### 5.3.1 Provider Integrated Display

The *Provider Integrated Display* Tab displays the Business Trust Summary and the Security Maturity Summary side-by-side for comparison between providers (Figure 45). This is the only integrated display of individual providers; the other integrated displays depict decision alternatives. Although decisions are made between the available decision alternatives, this is a convenient display to compare and contrast how individual providers contribute to the decision alternatives.

Provider ID		Business Trust Assessment Scoring Summary				Security Maturity Assessment Scoring Summary			
Provider ID	Provider	Overall Business Trust Score	Business Trust Basis Level	Business Trust Level ID	Rank Order	Overall Security Maturity Score	Security Maturity Level	Security Maturity Level ID	Rank Order
2	Self Now 12/18/19	0.91	Level 4 - High Trust Basis	4	3	0.65	Level 2 - Defined, Limited Scope	2	3
3	Self Future 12/18/19	0.92	Level 4 - High Trust Basis	4	2	0.67	Level 2 - Defined, Limited Scope	2	2
4	Alpha Inc. 12/18/19	0.95	Level 5 - Very High Trust Basis	5	1	0.46	Level 1 - Undefined, Undocumented	1	4
5	Bravo Inc. 12/18/19	0.73	Level 2 - Low Trust Basis	2	4	0.20	Level 1 - Undefined, Undocumented	1	6
6	Charlie Inc. 12/18/19	0.62	Level 2 - Low Trust Basis	2	6	0.95	Level 5 - Corporate Optimization	5	1
7	Delta Inc. 12/18/19	0.69	Level 2 - Low Trust Basis	2	5	0.40	Level 1 - Undefined, Undocumented	1	5
8	Echo Inc. 12/18/19	0.27	Level 1 - Very Low Trust Basis	1	7	0.00	Insufficient Evidence	0	8
9	Foxtrot Inc. 12/18/19	0.00	Insufficient Evidence	0	8	0.16	Insufficient Evidence	0	7

Figure 45: Provider Integrated Display

Key information available from the display:

- Alpha Inc. scored very high in Business Trust but very low in Security Maturity; whereas, Charlie Inc. scored low in Business Trust but very high in Security Maturity.
- Alpha Inc. is ranked first in Business Trust and fourth in Security Maturity.
- Charlie is ranked first in Security Maturity and sixth in Business Trust.
- Self Future is ranked second in both Business Trust and Security Maturity however, it’s Security Maturity is at Level 2, two levels below top ranked Charlie Inc.
- Echo Inc. is seventh in Business Trust and eighth in Security Maturity; Foxtrot Inc. is eighth in Business Trust and seventh in Security Maturity.

Review of the information in the *Provider Integrated Display* Tab prompts the need for additional analysis. For example:

- Researching whether modifying the default of equal value weights assigned to Business Trust and Security Maturity (i.e. modifying allocation of risk tolerance) would significantly change the rank order of decision alternatives.
- Examining the provider participants and their scores can provide insight into how the decision alternatives became “racked and stacked” in the next set of displays.



### 5.3.2 Decision Alternative Business Display

Up to this point, the ONSAT displays have focused primarily on summarizing the assessment of the *providers* that make up the decision alternatives. The remaining displays provide a direct comparison of the *decision alternatives* to support decision-makers.

The first of these decision alternative comparison displays is the *Decision Alternative Business Display* Tab (Figure 46). This display shows the Aggregated Business Trust Score for each of the decision alternatives as well as the Business Trust Score for each of the component providers. The Aggregated Business Trust Score for each decision alternative is used along with the associated Aggregated Security Maturity Score and Aggregated Financial Cost Score to develop an Aggregated Total Value Score. For each decision alternative, the percentage distribution of the Aggregated Business Trust Score across the Business Trust Categories is also included.

Decision Alternative			Alternative Providers			Business Trust Assessment Scoring			Provider Input to Decision Alternative			Distribution of Category Levels						
Rank Order	Alt #	Decision Alternative	Self	Prime	Sub	Business Trust Score	Business Trust Level	Business Trust Level ID	Self	Prime	Sub	Not Applicable	0.95	0.85	0.75	0.50	0.20	0.00
													Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 2 - Low Trust Basis	Level 1 - Very Low Trust Basis	Inadequate Evidence
2	1	Decision Alt. A - 12/18/2019	Self Now			0.91	Level 4 - High Trust Basis	4	0.91			23%	68%	3%	5%	1%		
1	2	Decision Alt. B - 12/18/2019	Self Future	Alpha Inc.		0.93	Level 4 - High Trust Basis	4	0.92	0.95		11%	84%	3%	2%			
3	3	Decision Alt. C - 12/18/2019	Self Future	Alpha Inc.	Delta Inc.	0.85	Level 4 - High Trust Basis	4	0.92	0.95	0.69	10%	66%	7%	7%	6%	3%	2%
9	4	Decision Alt. D - 12/18/2019	Self Future	Alpha Inc.	Echo Inc.	0.71	Level 2 - Low Trust Basis	2	0.92	0.95	0.27	11%	60%	2%	1%		23%	4%
11	5	Decision Alt. E - 12/18/2019	Self Future	Alpha Inc.	Foxtrot Inc.	0.62	Level 2 - Low Trust Basis	2	0.92	0.95	0.00	8%	56%	2%	1%			33%
4	6	Decision Alt. F - 12/18/2019	Self Future	Bravo Inc.		0.82	Level 3 - Moderate Trust Basis	3	0.92	0.73		11%	43%	33%	2%		11%	
6	7	Decision Alt. G - 12/18/2019	Self Future	Bravo Inc.	Delta Inc.	0.78	Level 3 - Moderate Trust Basis	3	0.92	0.73	0.69	10%	38%	27%	7%	6%	10%	2%
10	8	Decision Alt. H - 12/18/2019	Self Future	Bravo Inc.	Echo Inc.	0.64	Level 2 - Low Trust Basis	2	0.92	0.73	0.27	11%	32%	22%	1%		31%	4%
14	9	Decision Alt. I - 12/18/2019	Self Future	Bravo Inc.	Foxtrot Inc.	0.55	Level 2 - Low Trust Basis	2	0.92	0.73	0.00	8%	28%	22%	1%		8%	33%
7	10	Decision Alt. J - 12/18/2019	Self Future	Charlie Inc.		0.77	Level 3 - Moderate Trust Basis	3	0.92	0.62		11%	46%	3%	25%		8%	7%
8	11	Decision Alt. K - 12/18/2019	Self Future	Charlie Inc.	Delta Inc.	0.74	Level 2 - Low Trust Basis	2	0.92	0.62	0.69	10%	40%	7%	22%	6%	8%	7%
12	12	Decision Alt. L - 12/18/2019	Self Future	Charlie Inc.	Echo Inc.	0.60	Level 2 - Low Trust Basis	2	0.92	0.62	0.27	11%	34%	2%	16%		28%	8%
15	13	Decision Alt. M - 12/18/2019	Self Future	Charlie Inc.	Foxtrot Inc.	0.51	Level 2 - Low Trust Basis	2	0.92	0.62	0.00	8%	31%	2%	16%		5%	38%
5	14	Decision Alt. N - 12/18/2019	Self Future		Delta Inc.	0.80	Level 3 - Moderate Trust Basis	3	0.92		0.69	15%	49%	10%	11%	9%	4%	3%
13	15	Decision Alt. O - 12/18/2019	Self Future		Echo Inc.	0.60	Level 2 - Low Trust Basis	2	0.92		0.27	16%	39%	3%	2%		35%	5%

Figure 46: Decision Alternative Business Display

Key information available from the display:

- The only decision alternative that has a higher score than continuing to perform the services in-house (Self Now) is Decision Alternative B that outsources to Alpha Inc.
- If the outsourcing decision were based solely on Business Trust, Alternative B or retaining in-house would be the two best options.
- The *Decision Alternative Business Display* Tab confirms information gleaned from the provider business displays. With the exception of Decision Alternative B, all other decision alternatives

that include a prime (Decision Alternatives F and J), or a sub acting as a prime (Decision Alternatives N and O), lower the Aggregated Total Business Trust Score.

- Continuing this trend, all decision alternatives that include a sub have a lower Aggregated Total Business Trust Score than the alternatives that include only a prime (Figure 46A).

Rank Order	Alt #	Decision Alternative	Self	Prime	Sub	Business Trust Score	Business Trust Level	Business Trust Level ID	Self	Prime	Sub
2	1	Decision Alt. A	Self Now			0.91	High Trust	4	0.91		
1	2	Decision Alt. B	Self Future	Alpha Inc.		0.93	High Trust	4	0.92	0.95	
11	5	Decision Alt. E	Self Future	Alpha Inc.	Foxtrot Inc.	0.62	Low Trust	2	0.92	0.95	0.00
4	6	Decision Alt. F	Self Future	Bravo Inc.		0.82	Moderate Trust	3	0.92	0.73	
14	9	Decision Alt. I	Self Future	Bravo Inc.	Foxtrot Inc.	0.55	Low Trust	2	0.92	0.73	0.00
7	10	Decision Alt. J	Self Future	Charlie Inc.		0.77	Moderate Trust	3	0.92	0.62	
15	13	Decision Alt. M	Self Future	Charlie Inc.	Foxtrot Inc.	0.51	Low Trust	2	0.92	0.62	0.00

Figure 46A: Subs Lower Aggregated Business Trust Score

- The impact on the Aggregated Business Trust Scores varies e.g. the inclusion of Echo Inc. or Foxtrot Inc. as a sub lowers Aggregated Business Trust Score more than the inclusion of Delta Inc. as a sub.

Review of the information in the *Decision Alternative Business Display* Tab prompts the need for additional analysis. For example:

- Confirming that inclusion of Echo Inc. or Foxtrot Inc. as subs in a decision alternative does not significantly increase the security maturity (Section 5.3.3).
- Taking **A Closer Look** at those area(s) for which Decision Alternative A has a lower Aggregated Total Business Trust Score than Decision Alternative B to gain insight into Self Now’s specific Business Trust gaps.

*This is Blank Space*

*This is Blank Space*



**A CLOSER LOOK... Gap in Outsourcing Organization's Supply Chain Security**

According to the *Business Summary* Tab, Self Now scored lower than Alpha Inc. for 7 questions in the Business Trust Assessment.

- Of the 7 questions, 2 are in "Category E: Major Specific Requirements of Services to be Provided".
  - For 1 of the 2 questions (Question #50), Self Now scored **0.50** compared to Alpha Inc.'s score of **0.95**.
  - Self Now's low score for Question # 50 indicates a **GAP** in its' ability to meet major Supply Chain Security and Delivery Specifications and Requirements.

From Business Summary Tab					# of Questions at Each Rating Level						
Business Trust Assessment Comparison		Aggregated Total Value Business Scores			Not Applicable	5	4	3	2	1	0
ID #		Aggregated Total Value Score	Aggregated Total Value Level	Aggregated Total Value Level ID	Level 5 - Very High Trust Basis	Level 4 - High Trust Basis	Level 3 - Moderate Trust Basis	Level 2 - Low Trust Basis	Level 1 - Very Low Trust Basis	Insufficient Evidence	
2	Self Now	0.91	High Trust Basis	4	17	51	2	4	1		
4	Alpha Inc.	0.95	Very High Trust Basis	5	17	75					
<b>Self Now's High Trust Basis Masks Supply Chain Security Gap!</b>											
Business Trust					Self Now	Alpha Inc.					
Category E	MAJOR SPECIFIC REQUIREMENTS OF SERVICES TO BE PROVIDED				High Trust	Very High Trust					
Question 50	Assessment of Ability to Satisfy Major SUPPLY CHAIN SECURITY and Delivery Specifications / Requirements				Low Trust Score: 0.50	Very High Trust					

**Low Business Trust in Supply Chain Security is a Critical Gap**

Supply chain security and delivery for cloud storage encompasses not only procurement but also operation while in the cloud.<sup>1</sup> Thus, when selecting a service provider for cloud storage, the outsourcing organization needs to consider both business and technical aspects of risk management.

<sup>1</sup> NSA. (2020, January 22). Cybersecurity Mitigating Cloud Vulnerabilities. Retrieved May 16, 2020, from [https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES\\_20200121.PDF](https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF)

5.3.3 Decision Alternative Security Display

The *Decision Alternative Security Display* Tab shows the Aggregated Security Maturity Score for each of the decision alternatives as well as the Security Maturity Score for each of the component providers (Figure 47, next page). The Aggregated Total Security Maturity Score for each decision alternative is used along with the associated Aggregated Total Business Trust and Aggregated Total Financial Cost Utility Scores to develop an Aggregated Total Value Score. For each decision alternative, the percentage distribution of the Aggregated Total Security Maturity Score across the Security Categories is also included.

Key information available from the display:

- The sole decision alternative with a Security Maturity Score at or above the Corporate Standard Level is Decision Alternative J that outsources to Charlie Inc.; all other decision alternatives are in Security Maturity Level 1 or Level 2.

Decision Alternatives			Alternative Providers			Security Maturity Assessment Scoring			Provider Input to Decision Alternative			Distribution of Category Levels						
Rank Order	Alt #	Decision Alternative	Self	Prime	Sub	Security Maturity Score	Security Maturity Level	Security Maturity Level ID	Self	Prime	Sub	Not Applicable	0.95	0.85	0.75	0.50	0.20	0.00
													Level 5 - Corporate Optimization	Level 4 - Quantitatively Managed	Level 3 - Corporate Standard	Level 2 - Defined, Limited Scope	Level 1 - Undefined, Undocumented	Insufficient Evidence
3	1	Decision Alt. A - 12/18/2019	Self Now			0.65	Level 2 - Defined, Limited Scope	2	0.65				11%	13%	32%	34%	9%	0%
5	2	Decision Alt. B - 12/18/2019	Self Future	Alpha Inc.		0.56	Level 2 - Defined, Limited Scope	2	0.67	0.46			6%	18%	27%	24%	14%	10%
8	3	Decision Alt. C - 12/18/2019	Self Future	Alpha Inc.	Delta Inc.	0.51	Level 2 - Defined, Limited Scope	2	0.67	0.46	0.40		4%	12%	18%	43%	10%	13%
12	4	Decision Alt. D - 12/18/2019	Self Future	Alpha Inc.	Echo Inc.	0.38	Level 1 - Undefined, Undocumented	1	0.67	0.46	0.00		4%	12%	18%	16%	10%	40%
10	5	Decision Alt. E - 12/18/2019	Self Future	Alpha Inc.	Foxtrot Inc.	0.43	Level 1 - Undefined, Undocumented	1	0.67	0.46	0.16		4%	12%	18%	16%	36%	13%
9	6	Decision Alt. F - 12/18/2019	Self Future	Bravo Inc.		0.43	Level 1 - Undefined, Undocumented	1	0.67	0.20			6%	8%	17%	14%	54%	0%
11	7	Decision Alt. G - 12/18/2019	Self Future	Bravo Inc.	Delta Inc.	0.42	Level 1 - Undefined, Undocumented	1	0.67	0.20	0.40		4%	5%	11%	36%	36%	7%
15	8	Decision Alt. H - 12/18/2019	Self Future	Bravo Inc.	Echo Inc.	0.29	Level 1 - Undefined, Undocumented	1	0.67	0.20	0.00		4%	5%	11%	10%	36%	33%
13	9	Decision Alt. I - 12/18/2019	Self Future	Bravo Inc.	Foxtrot Inc.	0.34	Level 1 - Undefined, Undocumented	1	0.67	0.20	0.16		4%	5%	11%	10%	63%	7%
1	10	Decision Alt. J - 12/18/2019	Self Future	Charlie Inc.		0.81	Level 3 - Corporate Standard	3	0.67	0.95			56%	8%	17%	14%	4%	0%
2	11	Decision Alt. K - 12/18/2019	Self Future	Charlie Inc.	Delta Inc.	0.67	Level 2 - Defined, Limited Scope	2	0.67	0.95	0.40		37%	5%	11%	36%	3%	7%
6	12	Decision Alt. L - 12/18/2019	Self Future	Charlie Inc.	Echo Inc.	0.54	Level 2 - Defined, Limited Scope	2	0.67	0.95	0.00		37%	5%	11%	10%	3%	33%
4	13	Decision Alt. M - 12/18/2019	Self Future	Charlie Inc.	Foxtrot Inc.	0.59	Level 2 - Defined, Limited Scope	2	0.67	0.95	0.16		37%	5%	11%	10%	30%	7%
7	14	Decision Alt. N - 12/18/2019	Self Future		Delta Inc.	0.53	Level 2 - Defined, Limited Scope	2	0.67		0.40		6%	8%	17%	54%	4%	10%
14	15	Decision Alt. O - 12/18/2019	Self Future		Echo Inc.	0.33	Level 1 - Undefined, Undocumented	1	0.67		0.00		6%	8%	17%	14%	4%	50%

Figure 47: Decision Alternative Security Display

Key information available from the display, *Continued*:

- Unlike Self Now’s high Business Trust Score of .91; it’s Security Maturity Score of .65 falls within Level 2, Defined and Limited Scope.
- If the outsourcing decision were based solely on Security Maturity, Alternative J would be the sole candidate.
- With the exception of decision alternative J, all other decision alternatives that include a prime (B, F) or a sub acting as a prime (N, O) negatively impact the Aggregated Security Maturity Score.
- Similar to Business Trust, all decision alternatives that include a sub have a lower Aggregated Security Maturity Score than the alternatives that include only a prime; and, inclusion of Delta Inc. has less of an impact than Echo Inc. or Foxtrot Inc. (Figure 47A).

Rank Order	Alt #	Decision Alternative	Self	Prime	Sub	Security Maturity Score	Security Maturity Level	Security Maturity Level ID	Self	Prime	Sub
1	10	Decision Alt. J	Self Future	Charlie Inc.		0.81	Corporate Standard	3	0.67	0.95	
2	11	Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.	0.67	Defined, Limited Scope	2	0.67	0.95	0.40
6	12	Decision Alt. L	Self Future	Charlie Inc.	Echo Inc.	0.54	Defined, Limited Scope	2	0.67	0.95	0.00
4	13	Decision Alt. M	Self Future	Charlie Inc.	Foxtrot Inc.	0.59	Defined, Limited Scope	2	0.67	0.95	0.16

Figure 47A: Subs in Decision Alternatives Lowers Aggregated Security Maturity Score

Review of the information in the *Decision Alternative Security Display* Tab prompts the need for additional analysis. For example:

- Exploring potential of leveraging Charlie Inc.’s security practices in an outsourcing arrangement and whether those practices can be emulated by the outsourcing organization to improve its internal security practices.
- Examining if Bravo Inc.’s extremely low Security Maturity Score of 0.20 may have placed Bravo Inc. into an “unacceptable” level of risk to the outsourcing organization. Delta Inc. acting as a prime is in only a slightly better position based on its Security Maturity Score of 0.40.
- As the outsourcing organization, exploring whether it is more cost effective to resolve internal areas identified as weak in security maturity or to outsource to a provider that has a higher Security Maturity Level and thus, higher trustworthiness in those same areas.

### 5.3.4 Decision Alternative Financial Display

Similar to both the Business Trust and Security Maturity Decision Alternative Displays, the Decision Alternative Financial Display shows the Aggregated Financial Cost Scores for each of the alternatives. It also shows the aggregated Financial Costs in U.S. dollars (Figure 48). Unlike the previous two displays, it does not show the costs of the individual providers. Those are displayed on the *Financial Summary* Tab (Section 5.2.3).

Decision Alternative		Alternative Participants			Financial Assessment Scoring			Financial Cost	
Rank Order	Alt #	Decision Alternative	Self	Prime	Sub	Financial Cost Utility Score	Financial Cost Level	Financial Cost Level ID	Decision Alternative Cost \$M
15	1	Decision Alt. A 12/18/2019	Self Now			0.03	Level 1 - Very High Cost Alternative	★ 1	\$ 17.5 (M)
1	2	Decision Alt. B 12/18/2019	Self Future	Alpha Inc.		0.44	Level 5 - Very Low Cost Alternative	5	\$ 10.0 (M)
1	3	Decision Alt. C 12/18/2019	Self Future	Alpha Inc.	Delta Inc.	0.44	Level 5 - Very Low Cost Alternative	5	\$ 10.0 (M)
1	4	Decision Alt. D 12/18/2019	Self Future	Alpha Inc.	Echo Inc.	0.44	Level 5 - Very Low Cost Alternative	5	\$ 10.0 (M)
1	5	Decision Alt. E 12/18/2019	Self Future	Alpha Inc.	Foxtrot Inc.	0.44	Level 5 - Very Low Cost Alternative	5	\$ 10.0 (M)
7	6	Decision Alt. F 12/18/2019	Self Future	Bravo Inc.		0.33	Level 4 - Low Cost Alternative	4	\$ 12.0 (M)
7	7	Decision Alt. G 12/18/2019	Self Future	Bravo Inc.	Delta Inc.	0.33	Level 4 - Low Cost Alternative	4	\$ 12.0 (M)
7	8	Decision Alt. H 12/18/2019	Self Future	Bravo Inc.	Echo Inc.	0.33	Level 4 - Low Cost Alternative	4	\$ 12.0 (M)
7	9	Decision Alt. I 12/18/2019	Self Future	Bravo Inc.	Foxtrot Inc.	0.33	Level 4 - Low Cost Alternative	4	\$ 12.0 (M)
11	10	Decision Alt. J 12/18/2019	Self Future	Charlie Inc.		0.22	Level 3 - Moderate Cost Alternative	3	\$ 14.0 (M)
11	11	Decision Alt. K 12/18/2019	Self Future	Charlie Inc.	Delta Inc.	0.22	Level 3 - Moderate Cost Alternative	3	\$ 14.0 (M)
11	12	Decision Alt. L 12/18/2019	Self Future	Charlie Inc.	Echo Inc.	0.22	Level 3 - Moderate Cost Alternative	3	\$ 14.0 (M)
11	13	Decision Alt. M 12/18/2019	Self Future	Charlie Inc.	Foxtrot Inc.	0.22	Level 3 - Moderate Cost Alternative	3	\$ 14.0 (M)
6	14	Decision Alt. N 12/18/2019	Self Future		Delta Inc.	0.36	Level 4 - Low Cost Alternative	4	\$ 11.5 (M)
5	15	Decision Alt. O 12/18/2019	Self Future		Echo Inc.	0.42	Level 5 - Very Low Cost Alternative	5	\$ 10.5 (M)

Figure 48: Decision Alternative Financial Display

Key information available from the display:

- All decision alternatives fall below the maximum budget of \$18 (M).
- Decision Alternative A, Self Now, represents the option to not outsource and has the highest Financial Cost.
- The other fourteen Decision Alternatives are grouped into 1 of 3 Cost Levels:
  - Decision Alternatives B, C, D, E, and O are in Group 1: Very Low Cost Alternative.
  - Decision Alternatives F, G, H, I, and N are in Group 2: Low Cost Alternative.
  - Decision Alternatives J, K, L, and M are in Group 3: Moderate Cost Alternative.
- From a solely Financial Cost perspective, any of the outsourcing alternatives is better than continuing to provide these services internally.
- The primary cost difference between the decision alternatives is driven by the cost differences between the primes or a sub acting as a prime in each alternative.
- Bravo Inc.'s Financial Cost in Decision Alternative F makes this option competitive against Decision Alternative J in which Charlie Inc. is the prime.
- Decision Alternatives N and O, in which Delta Inc. and Echo Inc. are subs acting as a prime, are financially well positioned against Decision Alternative J.
- Inclusion of a sub in a decision alternative does not impact the Financial Cost.

Review of the information in the *Decision Alternative Financial Display* Tab prompts the need for additional analysis. For example:

- Checking internal guidance to verify if there is a Financial Cost limit or preferred range specific to this outsourcing scenario (beyond the maximum budget used in the Financial Assessment).
  - For this scenario, internal guidance confirmed that any decision alternative for which the Financial Cost is a minimum of 20% less than the outsourcing organization's current cost is "acceptable" i.e. a Financial Cost equal to or less than \$14.0 (M) is "acceptable".
  - Thus, all Decision Alternatives, other than Decision Alternative A (maintaining in-house), have an "acceptable" Financial Cost.
- With the focus of the outsourcing decision primarily resting on Business Trust and Security Maturity, the removal of certain decision alternatives from additional consideration is possible.
  - Eliminating Decision Alternatives in which Echo Inc. (Alternatives D, H, and L) or Foxtrot Inc. (Alternatives E, I, and M) are subs.
    - All six of these decision alternatives have a lower Aggregated Business Trust Score and a lower Aggregated Security Maturity Score than the decision alternatives with solely a prime. Delta Inc. as a sub will be examined in the next Section.

**Intermediate Decision:**



**Eliminating ALL Decision Alternatives comprised of Subs Echo Inc. or Foxtrot Inc. from Additional Consideration**

- Eliminating Decision Alternative O for in which Echo Inc. is the prime.
  - Decision Alternative O is financially competitive; however, as the prime, Echo Inc.'s very low Business Trust Score (0.27) and its non-existent Security Maturity Score (0.0), significantly raises the risk level for the outsourcing organization.



**Intermediate Decision:**

**Eliminating Decision Alternative O comprised of Echo Inc. (sub acting as a prime) from Additional Consideration**

- With elimination of the above, there are eight decision alternatives remaining (Figure 48A).

Rank Order	Decision Alternative		Alternative Participants			Financial Assessment Scoring			Financial Cost
	Alt #	Decision Alternative	Self	Prime	Sub	Financial Cost Utility Score	Financial Cost Level	Financial Cost Level ID	Decision Alternative Cost \$M
15	1	Decision Alt. A	Self Now			★ 0.03	Very High Cost Alternative	1	\$ 17.5 (M)
1	2	Decision Alt. B	Self Future	Alpha Inc.		0.44	Very Low Cost Alternative	5	\$ 10.0 (M)
1	3	Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.	0.44	Very Low Cost Alternative	5	\$ 10.0 (M)
7	6	Decision Alt. F	Self Future	Bravo Inc.		0.33	Low Cost Alternative	4	\$ 12.0 (M)
7	7	Decision Alt. G	Self Future	Bravo Inc.	Delta Inc.	0.33	Low Cost Alternative	4	\$ 12.0 (M)
11	10	Decision Alt. J	Self Future	Charlie Inc.		0.22	Moderate Cost Alternative	3	\$ 14.0 (M)
11	11	Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.	0.22	Moderate Cost Alternative	3	\$ 14.0 (M)
6	14	Decision Alt. N	Self Future		Delta Inc.	0.36	Low Cost Alternative	4	\$ 11.5 (M)

Figure 48A: Eight Decision Alternatives Remaining after Decision Alternative Financial Display

- Determining if there are any potential cost savings associated with a prime using different subs.
  - In the example, the prime’s Financial Cost includes all sub costs; thus, the Financial Cost is constant across all decision alternatives with the same prime regardless of the sub participant. Exploring this opportunity with the prime is not covered in this user manual.

**Note to User:**  
 The *Decision Alternative Score Summary* Tab, the *Decision Alternative Integrated Display* Tab and the *Total Value (Ranked)* Tab have a menu box at the top of the tab (below).

Display of Top X Alternatives    15

- This menu box enables a user to enter the number of decision alternatives to be displayed in rank order by Aggregated Total Value Score.
- Ranking is based on all Assessment Criteria (Business Trust, Security Maturity, and Financial Cost) weighted equally (*Weighting the three criteria differently will change the Aggregated Total Value Scores and thus, the rank order*).
- Using the display menu box provides insight and lends structure for presentations but should not be leveraged as the sole constraint in evaluation or scoping of the decision alternatives.

### 5.3.5 Decision Alternative Score Summary

Analysis of Decision Alternatives in the three previous displays focused separately on Business Trust, Security Maturity, and Financial Cost. The *Decision Alternative Score Summary* Tab is a comprehensive summary display. This display enables analysts to see a summary of the Aggregated Total Value, Aggregated Total Business Trust, Aggregated Total Security Maturity, and Aggregated Total Financial Cost information. Users can also scroll to view and identify significant categories and questions that contribute to these aggregated scores (Figure 49, next page). The *Decision Alternative Score Summary* Tab is a straightforward numerical display for analysis that is also beneficial for high-level comparisons and presentations to decision managers.



Display Top X Alternatives		15			Total Score	Decision Alternative Summary Scores			Cost (\$)		
Decision Alternatives		Alternative Providers			Aggregated Total Value Score	Aggregated Total Business Trust Score	Aggregated Total Security Maturity Score	Aggregated Total Financial Cost Score	Aggregated Total Financial Cost		
Location in the tool					Default Importance Weights =>						
					Swing Weights =>						
Best =>		Rank Order	Decision Alternative	SELF	PRIME	SUB	Best =>				
Worst =>							Worst =>				
Location in the manual											
6	Decision Alt. A	Self Now					☆ 0.53	0.91	0.65	0.03	\$ 17.5 (M)
1	Decision Alt. B	Self Future	Alpha Inc.				0.65	0.93	0.56	0.44	\$ 10.0 (M)
2	Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.			0.60	0.85	0.51	0.44	\$ 10.0 (M)
9	Decision Alt. D	Self Future	Alpha Inc.	Echo Inc.			0.51	0.71	0.38	0.44	\$ 10.0 (M)
10	Decision Alt. E	Self Future	Alpha Inc.	Foxtrot Inc.			0.50	0.62	0.43	0.44	\$ 10.0 (M)
7	Decision Alt. F	Self Future	Bravo Inc.				0.53	0.82	0.43	0.33	\$ 12.0 (M)
8	Decision Alt. G	Self Future	Bravo Inc.	Delta Inc.			0.51	0.78	0.42	0.33	\$ 12.0 (M)
14	Decision Alt. H	Self Future	Bravo Inc.	Echo Inc.			0.42	0.64	0.29	0.33	\$ 12.0 (M)
15	Decision Alt. I	Self Future	Bravo Inc.	Foxtrot Inc.			0.41	0.55	0.34	0.33	\$ 12.0 (M)
3	Decision Alt. J	Self Future	Charlie Inc.				0.60	0.77	0.81	0.22	\$ 14.0 (M)
5	Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.			0.55	0.74	0.67	0.22	\$ 14.0 (M)
11	Decision Alt. L	Self Future	Charlie Inc.	Echo Inc.			0.45	0.60	0.54	0.22	\$ 14.0 (M)
13	Decision Alt. M	Self Future	Charlie Inc.	Foxtrot Inc.			0.44	0.51	0.59	0.22	\$ 14.0 (M)
4	Decision Alt. N	Self Future		Delta Inc.			0.57	0.80	0.53	0.36	\$ 11.5 (M)
12	Decision Alt. O	Self Future		Echo Inc.			0.45	0.60	0.33	0.42	\$ 10.5 (M)

Figure 49: Decision Alternative Score Summary

Key information available from the display:

- The display is in order by Decision Alternative with the rank order for each alternative to the left of the Decision Alternative name.
- New to this display are the Aggregated Total Value Scores for each Decision Alternative.
- The top two rows of scores contain the *Best* and *Worst* Aggregated Total Value Scores, followed by the *Best* and *Worst* Scores for Aggregated Total Business Trust Score, Aggregated Total Security Maturity Score, and Aggregated Total Financial Cost Utility Score. The *Best* and *Worst* Financial Cost is reflected in the last column.
- The best Aggregated Total Value Score of 0.65 belongs to Decision Alternative B.
- Next highest are Decision Alternatives C and J that have the same Aggregated Total Value Score (0.60) but differ considerably in their Business Trust, Security Maturity, and Financial Cost.
- The Decision alternatives with the highest Aggregated Total Business Trust Score and the highest Aggregated Total Security Maturity Score do *not* have the same component providers.
- The ranges (high to low) across the first three sets of scores are as follows:
  - Aggregated Total Value Score: 0.65 (Alternative B) to 0.41 (Alternative I)
  - Aggregated Total Business Trust Score: 0.93 (Alternative B) to 0.51 (Alternative M)
  - Aggregated Total Security Maturity Score: 0.81 (Alternative J) to 0.29 (Alternative H)
- The elimination of Decision Alternatives H, I, and M from additional consideration is validated as these three alternatives represent the lowest end of the score ranges.

- Directly above the *Best* and *Worst* Scores, are the Default Importance Weights which are set to the default of equally weighting Business Trust, Security Maturity, and Financial Cost. Review of the information in the *Decision Alternative Score Summary* Tab prompts the need for additional analysis. For example:

- Verifying internal guidance on a minimum threshold set for Business Trust and/ or Security Maturity scores for potential service providers.
  - Minimum thresholds for Business Trust and Security Maturity can help scope the alternatives to align with the outsourcing organization’s current self-assessment and risk posture.
- Examining Delta Inc.’s inclusion as a sub in Decision Alternatives C, G, and K (Figure 49A).
  - The Aggregated Total Value Score of these three alternatives ranges from 0.60 to 0.51. Although this is a small range, Alternative G’s score is lower than the outsourcing organization and its’ Aggregated Total Security Maturity Score is in Level 1.

Rank Order	Decision Alternative	Alternative Providers			Aggregated Total Value Score (100%)	Aggregated Total Business Trust Score (33%)	Aggregated Total Security Maturity Score (33%)	Aggregated Total Financial Cost Score (33%)	Aggregated Total Financial Cost (33%)
		Self	PRIME	SUB					
6	Decision Alt. A	Self Now			★ 0.53	0.91	0.65	0.03	\$ 17.5 (M)
1	Decision Alt. B	Self Future	Alpha Inc.		0.65	0.93	0.56	0.44	\$ 10.0 (M)
2	Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.	0.60	0.85	0.51	0.44	\$ 10.0 (M)
7	Decision Alt. F	Self Future	Bravo Inc.		0.53	0.82	0.43	0.33	\$ 12.0 (M)
8	Decision Alt. G	Self Future	Bravo Inc.	Delta Inc.	0.51	0.78	0.42	0.33	\$ 12.0 (M)
3	Decision Alt. J	Self Future	Charlie Inc.		0.60	0.77	0.81	0.22	\$ 14.0 (M)
5	Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.	0.55	0.74	0.67	0.22	\$ 14.0 (M)
4	Decision Alt. N	Self Future		Delta Inc.	0.57	0.80	0.53	0.36	\$ 11.5 (M)

Figure 49A: Delta Inc. as a Sub

- Eliminating Decision Alternative G comprised of Bravo Inc. as the prime and Delta Inc. as the sub from additional consideration. Delta’s participation as a sub in Decision Alternative C and K will be examined for elimination in Section 5.4.

**Intermediate Decision:**

**Eliminating Decision Alternative G comprised of Delta Inc. as the sub from Additional Consideration**

- Continuing focus on the Business Trust and Security Maturity Scores in remaining decision alternatives as a method to complement the outsourcing organization’s strengths and gaps.
- With elimination of Decision Alternative G from additional consideration, there are seven decision alternatives remaining to vet (Figure 49B, next page).

Content for the remainder of Section 5 will continue to present all decision alternatives to demonstrate the use of the remaining two displays as well a validation of the intermediate decisions.

Rank Order	Decision Alternative	Alternative Providers			Aggregated Total Value Score (100%)	Aggregated Total Business Trust Score (33%)	Aggregated Total Security Maturity Score (33%)	Aggregated Total Financial Cost Score (33%)	Aggregated Total Financial Cost (33%)
		Self	PRIME	SUB					
6	Decision Alt. A	Self Now			★ 0.53	0.91	0.65	0.03	\$ 17.5 (M)
1	Decision Alt. B	Self Future	Alpha Inc.		0.65	0.93	0.56	0.44	\$ 10.0 (M)
2	Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.	0.60	0.85	0.51	0.44	\$ 10.0 (M)
7	Decision Alt. F	Self Future	Bravo Inc.		0.53	0.82	0.43	0.33	\$ 12.0 (M)
3	Decision Alt. J	Self Future	Charlie Inc.		0.60	0.77	0.81	0.22	\$ 14.0 (M)
5	Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.	0.55	0.74	0.67	0.22	\$ 14.0 (M)
4	Decision Alt. N	Self Future		Delta Inc.	0.57	0.80	0.53	0.36	\$ 11.5 (M)

Figure 49B: Seven Decision Alternatives Remaining for Additional Consideration

### 5.3.6 Decision Alternative Integrated Display

The *Decision Alternative Integrated Display* Tab and the *Total Value Display (Ranked)* Tab (Section 5.3.7) display the same decision alternative summary information. The only difference is that the *Decision Alternative Integrated Display* Tab (Figure 50, next page) shows the information in the order of the defined decisions alternatives and the *Total Value Display (Ranked)* Tab sorts the decision alternatives from best to worst based on the Aggregated Total Value Score.

Both the *Decision Alternative Integrated Display* Tab and the *Total Value (Ranked) Display* Tab are comprised of five sections (left to right):

- Decision alternative name, ID, and component providers,
- Aggregated Total Value Scores and Financial Cost for each decision alternative,
- Contributing Business Trust Scores for each decision alternative,
- Contributing Security Maturity Scores for each decision alternative, and,
- Financial Cost Utility Scores for each decision alternative.

*This is Blank Space*

Alternative #	Decision Alternative	Alternative Providers			Aggregated Total Value Scoring (100%)					Aggregated Business Trust Assessment Scoring (33%)			Aggregated Security Maturity Assessment Scoring (33%)			Aggregated Financial Cost Scoring		
		Self	Prime	Sub	Rank Order	Total Value Score	Total Value Level	Total Value Level ID	Decision Alternative Cost \$M	Business Trust Score	Business Trust Level	Business Trust Level ID	Security Maturity Score	Security Maturity Level	Security Maturity Level ID	Financial Cost Utility Score	Financial Cost Level	Financial Cost Level ID
1	A.	Self Now			6	0.53	Unsat	2	\$ 17.5 (M)	0.91	High Trust	4	0.65	Defined, Limited Scope	2	0.03	Very High Cost	1
2	B.	Self Future	Alpha Inc.		1	0.65	Unsat	2	\$ 10.0 (M)	0.93	High Trust	4	0.56	Defined, Limited Scope	2	0.44	Very Low Cost	5
3	C.	Self Future	Alpha Inc.	Delta Inc.	2	0.60	Unsat	2	\$ 10.0 (M)	0.85	High Trust	4	0.51	Defined, Limited Scope	2	0.44	Very Low Cost	5
4	D.	Self Future	Alpha Inc.	Echo Inc.	9	0.51	Unsat	2	\$ 10.0 (M)	0.71	Low Trust	2	0.38	Undefined, Undocumented	1	0.44	Very Low Cost	5
5	E.	Self Future	Alpha Inc.	Foxtrot Inc.	10	0.50	Highly Unsat	1	\$ 10.0 (M)	0.62	Low Trust	2	0.43	Undefined, Undocumented	1	0.44	Very Low Cost	5
6	F.	Self Future	Bravo Inc.		7	0.53	Unsat	2	\$ 12.0 (M)	0.82	Moderate Trust	3	0.43	Undefined, Undocumented	1	0.33	Low Cost	4
7	G.	Self Future	Bravo Inc.	Delta Inc.	8	0.51	Unsat	2	\$ 12.0 (M)	0.78	Moderate Trust	3	0.42	Undefined, Undocumented	1	0.33	Low Cost	4
8	H.	Self Future	Bravo Inc.	Echo Inc.	14	0.42	Highly Unsat	1	\$ 12.0 (M)	0.64	Low Trust	2	0.29	Undefined, Undocumented	1	0.33	Low Cost	4
9	I.	Self Future	Bravo Inc.	Foxtrot Inc.	15	0.41	Highly Unsat	1	\$ 12.0 (M)	0.55	Low Trust	2	0.34	Undefined, Undocumented	1	0.33	Low Cost	4
10	J.	Self Future	Charlie Inc.		3	0.60	Unsat	2	\$ 14.0 (M)	0.77	Moderate Trust	3	0.81	Corporate Standard	3	0.22	Moderate Cost	3
11	K.	Self Future	Charlie Inc.	Delta Inc.	5	0.55	Unsat	2	\$ 14.0 (M)	0.74	Low Trust	2	0.67	Defined, Limited Scope	2	0.22	Moderate Cost	3
12	L.	Self Future	Charlie Inc.	Echo Inc.	11	0.45	Highly Unsat	1	\$ 14.0 (M)	0.60	Low Trust	2	0.54	Defined, Limited Scope	2	0.22	Moderate Cost	3
13	M.	Self Future	Charlie Inc.	Foxtrot Inc.	13	0.44	Highly Unsat	1	\$ 14.0 (M)	0.51	Low Trust	2	0.59	Defined, Limited Scope	2	0.22	Moderate Cost	3
14	N.	Self Future		Delta Inc.	4	0.57	Unsat	2	\$ 11.5 (M)	0.80	Moderate Trust	3	0.53	Defined, Limited Scope	2	0.36	Low Cost	4
15	O.	Self Future		Echo Inc.	12	0.45	Highly Unsat	1	\$ 10.5 (M)	0.60	Low Trust	2	0.33	Undefined, Undocumented	1	0.42	Very Low Cost	5

Figure 50: Decision Alternative Integrated Display

Key information available from the display:

- This display provides a high-level synopsis of all the decision alternatives but can also mask insights important to the outsourcing decision.
- Additional insight and analysis related to the *Decision Alternative Integrated Display* Tab is discussed in Section 5.3.7: *Total Value Display (Ranked)*.

### 5.3.7 Total Value Display (Ranked)

The *Total Value Display (Ranked)* Tab contains the same information and information structure as the *Decision Alternative Integrated Display* Tab. The *Total Value Display (Ranked)* Tab displays the decision alternatives ranked from best to worst based on their Total Value Score (Figure 51, next page). Displaying decision alternatives in rank order affords analysts and decision makers an easy method for comparing the most competitive alternatives at a high level. Similar to the Decision Alternative Integrated Display, this display can mask insights important to the outsourcing decision.

Key information available from the display:

- Self Now has the highest Financial Cost (\$4 (M) higher than the next expensive decision alternative). The Financial Cost to retain in-house is cost prohibitive relative to other options.
- Validates the decision to remove the eight decision alternatives that score lower than Self Now.
- Five decision alternatives have a higher Aggregated Total Value Score than Self Now; one alternative has the same score.

Decision Alternative	Self	Prime	Sub	Rank Order (Unique)	Total Value Score	Total Value Level	Decision Alternative Cost (\$M)	Business Trust Score	Business Trust Level	Security Maturity Score	Security Maturity Level	Financial Cost Utility Score	Financial Cost Level
Decision Alt. B	Self Future	Alpha Inc.		1	0.65	Unsat Alternative	\$ 10.0 (M)	0.93	High Trust	0.56	Defined, Limited Scope	0.44	Very Low Cost
Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.	2	0.60	Unsat Alternative	\$ 10.0 (M)	0.85	High Trust	0.51	Defined, Limited Scope	0.44	Very Low Cost
Decision Alt. J	Self Future	Charlie Inc.		3	0.60	Unsat Alternative	\$ 14.0 (M)	0.77	Moderate Trust	0.81	Corporate Standard	0.22	Moderate Cost
Decision Alt. N	Self Future		Delta Inc.	4	0.57	Unsat Alternative	\$ 11.5 (M)	0.80	Moderate Trust	0.53	Defined, Limited Scope	0.36	Low Cost
Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.	5	0.55	Unsat Alternative	\$ 14.0 (M)	0.74	Low Trust	0.67	Defined, Limited Scope	0.22	Moderate Cost
Decision Alt. A	Self Now			6	0.53	Unsat Alternative	\$ 17.5 (M)	0.91	High Trust	0.65	Defined, Limited Scope	0.03	Very High Cost
Decision Alt. F	Self Future	Bravo Inc.		7	0.53	Unsat Alternative	\$ 12.0 (M)	0.82	Moderate Trust	0.43	Undefined, Undocumented	0.33	Low Cost
Decision Alt. G	Self Future	Bravo Inc.	Delta Inc.	8	0.51	Unsat Alternative	\$ 12.0 (M)	0.78	Moderate Trust	0.42	Undefined, Undocumented	0.33	Low Cost
Decision Alt. D	Self Future	Alpha Inc.	Echo Inc.	9	0.51	Unsat Alternative	\$ 10.0 (M)	0.71	Low Trust	0.38	Undefined, Undocumented	0.44	Very Low Cost
Decision Alt. E	Self Future	Alpha Inc.	Foxtrot Inc.	10	0.50	Highly Unsat Alternative	\$ 10.0 (M)	0.62	Low Trust	0.43	Undefined, Undocumented	0.44	Very Low Cost
Decision Alt. L	Self Future	Charlie Inc.	Echo Inc.	11	0.45	Highly Unsat Alternative	\$ 14.0 (M)	0.60	Low Trust	0.54	Defined, Limited Scope	0.22	Moderate Cost
Decision Alt. O	Self Future		Echo Inc.	12	0.45	Highly Unsat Alternative	\$ 10.5 (M)	0.60	Low Trust	0.33	Undefined, Undocumented	0.42	Very Low Cost
Decision Alt. M	Self Future	Charlie Inc.	Foxtrot Inc.	13	0.44	Highly Unsat Alternative	\$ 14.0 (M)	0.51	Low Trust	0.59	Defined, Limited Scope	0.22	Moderate Cost
Decision Alt. H	Self Future	Bravo Inc.	Echo Inc.	14	0.42	Highly Unsat Alternative	\$ 12.0 (M)	0.64	Low Trust	0.29	Undefined, Undocumented	0.33	Low Cost
Decision Alt. I	Self Future	Bravo Inc.	Foxtrot Inc.	15	0.41	Highly Unsat Alternative	\$ 12.0 (M)	0.55	Low Trust	0.34	Undefined, Undocumented	0.33	Low Cost

Figure 51: Total Value Display (Ranked)

- All seven of the remaining decision alternatives align with the Aggregated Total Value Level 2 (Unsatisfactory Alternative) which poses a challenge to the outsourcing organization in selecting an alternative that will maintain its strengths and fill its gaps.
- With the Financial Cost of all of the decision alternatives (except Alternative A) deemed “acceptable”, this display highlights important comparisons between Business Trust and Security Maturity (Figure 51A).
- For example, Decision Alternatives B and C ranked as #1 and #2 options both have a high Business Trust Level but a Low Security Maturity Level.
- The third option, Decision Alternative J has both a Level 3 Business Trust and Level 3 Security Maturity.
- If decision-makers want a provider to complement their organization’s low Security Maturity Level, the two best alternatives may no longer be the most risk smart.

Equally Weighted	Alternative Providers			Aggregated Business Trust Assessment Scoring (33%)		Aggregated Security Maturity Assessment Scoring (33%)		
	Decision Alternative	Self	Prime	Sub	Business Trust Score	Business Trust Level ID / Level	Security Maturity Score	Security Maturity Level ID / Level
	Decision Alt. B	Self Future	Alpha Inc.		0.93	(4) High Trust	0.56	(2) Defined, Limited Scope
	Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.	0.85	(4) High Trust	0.51	(2) Defined, Limited Scope
	Decision Alt. J	Self Future	Charlie Inc.		0.77	(3) Moderate Trust	0.81	Corporate Standard
	Decision Alt. N	Self Future		Delta Inc.	0.80	(3) Moderate Trust	0.53	(2) Defined, Limited Scope
	Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.	0.74	(2) Low Trust	0.67	(2) Defined, Limited Scope
	Decision Alt. A	Self Now			0.91	(4) High Trust	0.65	(2) Defined, Limited Scope
	Decision Alt. F	Self Future	Bravo Inc.		0.82	(3) Moderate Trust	0.43	(1) Undefined, Undocumented

Figure 51A: Business Trust and Security Maturity Comparison



Review of the information in the *Total Value Display (Ranked)* Tab prompts the need for additional analysis. For example:

- Researching minimum threshold for Security Maturity to align with the outsourcing organization’s current self-assessment, specifically gap areas.

### 5.3.8 Total Value Composite Chart

The *Total Value Composite Chart* is a graphical representation of the information from the *Total Value Display (Ranked)* Tab to help analysts and decision-makers visually compare and contrast the decision alternatives. This is a useful top level summary visualization to be used by analysts and decision-makers to guide decision discussions and exploration of the more detailed information to gain an in-depth understanding of the benefits and costs of the competing alternatives (Figure 52).

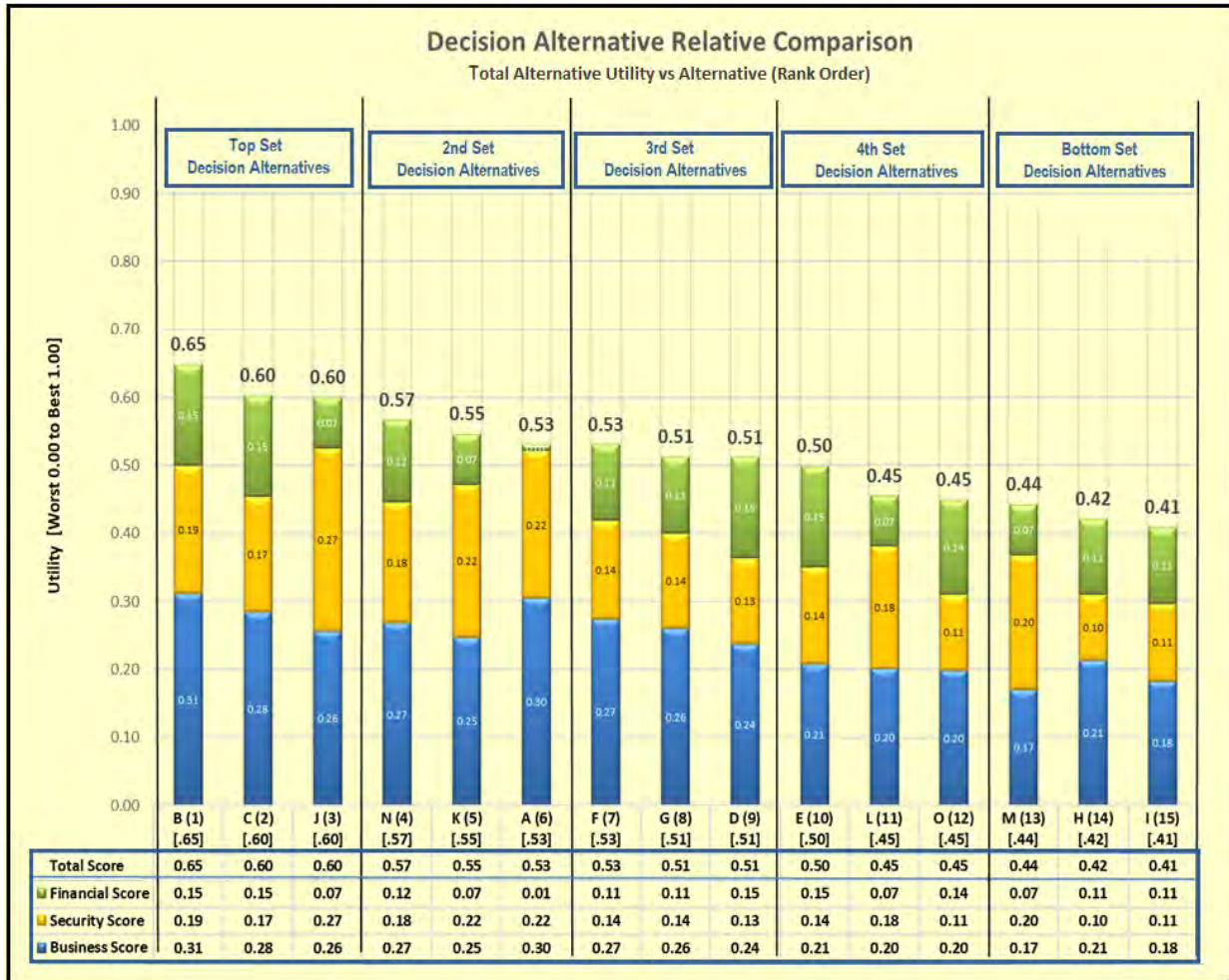


Figure 52: Total Value Composite Chart

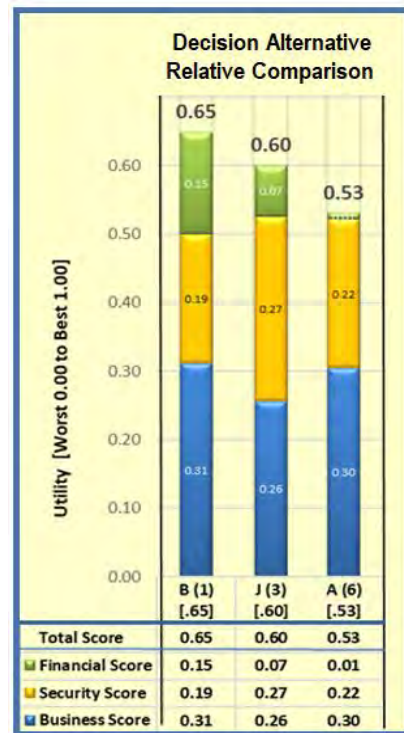
The decision alternatives are grouped into 5 ranked sets of 3 decision alternatives.

- Each bar represents the Aggregated Total Value Score of each alternative.
- Each bar is divided into the 3 component assessment criteria: Business Trust Score (Blue); Security Maturity Score (Gold); and Financial Cost Utility Score (Green).
- It should be noted that the score shown for each of the component elements is the normalized score which is the element’s score multiplied by the weight assigned to that component.

- Using Decision Alternative B as an example:  
The default equal value (33.33%) weight is applied to each component and the values would be as follows (values rounded to two decimal places):
  - Business Trust:  $(.93) \times (.33) = .31$
  - Security Maturity:  $(.56) \times (.33) = .19$
  - Financial Cost:  $(.44) \times (.33) = .15$
  - Total Value =  $(.31) + (.19) + (.15) = .65$

Key information available from the display:

- All decision alternatives are significantly under the 1.00 best overall utility score.
- Presents at a glance which of the criteria (Business Trust, Security Maturity, or Financial Cost) is providing the greatest contribution to a decision alternative's Aggregated Total Value Score.
  - Almost 50% of Decision Alternative J's Aggregated Total Value Score is contributed as Security Maturity.
  - Decision Alternative J has the largest Security Maturity contribution out of 15 decision alternatives.
  - Almost 50% of Decision Alternative B's Aggregated Total Value Score is contributed as Business Trust followed by Security Maturity and then Financial Cost.
  - Decision Alternative A, Self Now, has over 50% of its Aggregated Total Value Score contributed as Business Trust.



Review of the information in the *Total Value Composite Chart* prompts the need for additional analysis. For example:

- As part of Final Decision Support Analysis, modeling Security Maturity with a greater weight than Business Trust and Financial Cost. Specifically, examining whether it is more cost effective for the outsourcing organization to resolve internal areas identified as weak in security maturity or to outsource to a provider that has a higher Security Maturity Level and thus, higher trustworthiness in those same areas.
  - One way to vet this approach is to change the default criteria weights from equal for all three assessments to weight Security Maturity more than Business Trust and Financial Cost. An example of weighting Security Maturity at 45%, Business Trust at 30% and Financial Cost at 25% is discussed in Section 5.4.7

## 5.4 Final Decision Support Analysis

### 5.4.1 Overview of Deeper Analysis of the Top Decision Alternatives

Displays in Sections 5.1 and 5.2 focus on the strengths and gaps of the individual providers as components of the decision alternatives. The aggregated displays of decision alternatives in Section 5.3

leverage the Aggregated Total Value Score as the major criteria to compare and rank order the set of decision alternatives under consideration. Display descriptions across Section 5.0 also include example analysis tasks along with steps and rationale to consolidate the set of decision alternatives into a smaller set of top competitors. This section will leverage all of the insight and results garnered thus far to finalize a set of findings and recommendations to decision makers.

The seven decision alternatives remaining under consideration in our example are as follows:

- Current Operations [\$ 17.5 (M)]
  - Decision Alternative A - This will be used as a baseline in this final analysis.
- Two Decision Alternatives Using Alpha Inc. as the prime [\$10.0 (M)]
  - Decision Alternative B - Alpha Inc. with no sub
  - Decision Alternative C - Alpha Inc. with Delta Inc. as a sub
- Two Decision Alternatives with Charlie Inc. as the prime [\$ 14.0 (M)]
  - Decision Alternative J - Charlie Inc. with no sub
  - Decision Alternative K - Charlie Inc. with Delta Inc. as a sub
- One Decision Alternative with Bravo Inc. as the prime [\$12.0 (M)]
  - Decision Alternative F - Bravo Inc. with no sub
- One Decision Alternative Exploring Delta Inc. as a prime rather than a sub [\$ 11.5 (M)]
  - Decision Alternative N - Delta Inc.

#### 5.4.2 General Observations: Decision Alternatives Compared to Current Operations.

Current Operations (Alternative A) is used as a baseline to compare the other six decision alternatives. The following table (Figure 53) highlights the major differences between the options.

	Self	Self Now	Self Future	Self Future	Self Future	Self Future	Self Future	Self Future
	Prime		Alpha Inc.	Alpha Inc.	Charlie Inc.		Charlie Inc.	Bravo Inc.
	Sub			Delta Inc.		Delta Inc.	Delta Inc.	
	Decision Alternative	A	B	C	J	N	K	F
	Cost	\$ 17.5 (M)	\$ 10.0 (M)	\$ 10.0 (M)	\$ 14.0 (M)	\$ 11.5 (M)	\$ 14.0 (M)	\$ 12.0 (M)
	Aggregated Total Value Score	0.53	0.65	0.60	0.60	0.57	0.55	0.53
			+	+	+	+	+	
33%	Aggregated Total Business Trust Score	0.91	0.93	0.85	0.77	0.80	0.74	0.82
			+	-	-	-	-	-
33%	Aggregated Total Security Maturity Score	0.65	0.56	0.51	0.81	0.53	0.67	0.43
			-	-	+	-	-	-
33%	Aggregated Total Financial Cost Score	0.03	0.44	0.44	0.22	0.36	0.22	0.33
			+	+	+	+	+	+
	Savings		\$ 7.5 (M)	\$ 7.5 (M)	\$ 3.5 (M)	\$ 6.0 (M)	\$ 3.5 (M)	\$ 5.5 (M)
	# of Negatives		1	2	1	2	2	2

Figure 53: Comparison of Current Operations to Six Competing Decision Alternatives

All of the Aggregated Total Value Scores for decision alternatives in this comparison table, are in the Low Level 2 (Orange) range. All six of the outsourcing alternatives score as well or better than the current operational state; and therefore, there is benefit to reviewing these outsourcing alternatives to see whether or not the benefits are total cost effective from the decision-maker’s perspective.

From a Business Trust perspective, the current operations score is an area of strength for the outsourcing organization. Five of the decision alternatives do not score as well in Business Trust as current operations; one of these scores is still in Level 4 High Trust, three are within Level 3 Corporate Standard (yellow) and the lowest scoring alternative is in Level 2 Low Trust (Figure 53A). However, there is not a wide variation in scores (0.93 to 0.74). Notice that only Decision Alternative B improves upon the Business Trust of current operations.

33%	Self	Self Now	Self Future	Self Future	Self Future	Self Future	Self Future	Self Future
	Prime		Alpha Inc.	Alpha Inc.	Charlie Inc.		Charlie Inc.	Bravo Inc.
	Sub			Delta Inc.		Delta Inc.	Delta Inc.	
	Decision Alternative	A	B	C	J	N	K	F
	Aggregated Total Business Trust Score	0.91	0.93	0.85	0.77	0.80	0.74	0.82
			+	-	-	-	-	-

Figure 53A: Comparison of Aggregated Total Business Trust Scores

From a Security Maturity perspective, the current operations score is in Level 2 Defined, Limited Scope, indicating that this is a criteria area where it would be beneficial to select a partner that would improve the security posture of the network operations. Four of the alternatives score even lower than the current operations including one in the very low range. There is a wide variation in scores (0.81 to 0.43); in fact, the second highest score is 0.67. Note that only Decision Alternative J improves the Security Maturity of current operations.

33%	Self	Self Now	Self Future	Self Future	Self Future	Self Future	Self Future	Self Future
	Prime		Alpha Inc.	Alpha Inc.	Charlie Inc.		Charlie Inc.	Bravo Inc.
	Sub			Delta Inc.		Delta Inc.	Delta Inc.	
	Decision Alternative	A	B	C	J	N	K	F
	Aggregated Total Security Maturity Score	0.65	0.56	0.51	0.81	0.53	0.67	0.43
			-	-	+	-	-	-

Figure 53B: Comparison of Aggregated Total Security Maturity Scores

An ideal decision alternative is one that improves *both* Business Trust *and* Security Maturity of the outsourcing organization at an “acceptable” Financial Cost. In the set of available decision alternatives, all options provide a Financial Cost savings; but, unfortunately, there is *not* a single option that improves *both* Business Trust and Security Maturity (Figure 53C, next page). Thus, decision-makers are presented with the need to “trade-off” across the three criteria of Business Trust, Security Maturity, and Financial Cost. Additionally, the default equal weighting of the three criteria does not provide the necessary detail to the decision-makers to ensure an informed decision.



	Self	Self Now	Self Future	Self Future	Self Future	Self Future	Self Future	Self Future
	Prime		Alpha Inc.	Alpha Inc.	Charlie Inc.		Charlie Inc.	Bravo Inc.
	Sub			Delta Inc.		Delta Inc.	Delta Inc.	
	Decision Alternative	A	B	C	J	N	K	F
	Cost	\$ 17.5 (M)	\$ 10.0 (M)	\$ 10.0 (M)	\$ 14.0 (M)	\$ 11.5 (M)	\$ 14.0 (M)	\$ 12.0 (M)
33%	Aggregated Total Business Trust Score		+	-	-	-	-	-
33%	Aggregated Total Security Maturity Score		-	-	+	-	-	-
	# of Negatives		1	2	1	2	2	2

Figure 53C: No Single Decision Alternative Improves BOTH Business Trust AND Security Maturity

Section 5.4.7 details how to modify the decision criteria weights from the default settings using the *Decision Criteria – Weight Definition* Tab within the *Tool Adjustment Settings* Section. Results from weighting the decision criteria to align with the outsourcing organizations strengths and gaps should be included in the presentation to decision makers.

### 5.4.3 Additional Findings: Top Decision Alternatives Compared to Current Operations

There are some additional findings that can further reduce the current set of six decision alternatives to the two best options as compared to current operations. These findings confirm insights from previous displays in Section 5.0.

Aligning the six decision alternatives in rank order from the data displayed in *the Decision Score Summary* Tab helps visualize the best three options and the bottom three options. Two of the top three options outsource to primes (Alpha Inc. and Charlie Inc.) and one option outsources to a prime (Alpha Inc.) and a sub (Delta Inc.). The bottom three options are similar in that two options outsource to primes (Bravo Inc. and Delta Inc. acting as a prime) and one option outsources to a prime (Charlie Inc.) and a sub (Delta Inc.) (Figure 54).

Equally Weighted		Decision Alternative Summary Scores				Aggregated Total Value Score (100%)	Aggregated Total Business Trust Score (33%)	Aggregated Total Security Maturity Score (33%)	
		Alternative Providers							
Rank Order	Decision Alternative	Self	PRIME	SUB	Best =>	0.65	0.93	0.81	
					Worst =>	0.53	0.74	0.43	
6	Decision Alt. A	Self Now	Current Operations			★ 0.53	0.91	0.65	
1	Decision Alt. B	Self Future	Alpha Inc.				0.65	0.93	0.56
2	Decision Alt. C	Self Future	Alpha Inc.	Delta Inc.	Best 3	0.60	0.85	0.51	
3	Decision Alt. J	Self Future	Charlie Inc.			0.60	0.77	0.81	
4	Decision Alt. N	Self Future	Delta Inc.		Bottom 3	0.57	0.80	0.53	
5	Decision Alt. K	Self Future	Charlie Inc.	Delta Inc.		0.55	0.74	0.67	
7	Decision Alt. F	Self Future	Bravo Inc.			0.53	0.82	0.43	

Figure 54: Three Best and Three Worst Decision Alternatives

Outsourcing to a prime in the bottom three options:

- Decision Alternative F has the lowest Aggregated Security Maturity Score and ties with current operations for the lowest overall score. Bravo Inc.’s extremely low Security Maturity Score of 0.20 as the prime component of Decision Alternative F puts this option into the bin of “unacceptable” level of risk for the outsourcing organization and can be eliminated from final consideration.
- Decision Alternative N scores lower than current operations in both Business Trust and Security Maturity. In particular, Delta Inc.’s extremely low Security Maturity Score of 0.40 as the prime component of Decision Alternative N puts this option into the bin of “unacceptable” level of risk for the outsourcing organization and can be eliminated from final consideration.

Outsourcing to a prime and a sub:

- Delta Inc.’s inclusion as a sub with Alpha Inc. and Charlie Inc. as primes in Decision Alternatives C and K has a greater adverse impact on Security Maturity than on Business Trust, largely due to the benefit of aggregating Self Now’s high Business Trust Score and the detriment of aggregating Self Now’s very low Security Maturity Score (Figure 55). This aggregation difference when combined with a better Financial Cost Score is reflected in Decision Alternative C’s ranking in the top three options and Decision Alternative K’s ranking in the bottom three.
- Although the impact of Delta Inc. as a sub varies, there is not a benefit to include Delta Inc. as a sub in lieu of the corresponding Decision Alternatives B and J that outsource solely to the primes. This confirms a finding from Section 5.3 that all decision alternatives that include a sub have lower Aggregated Scores for Business Trust and Security Maturity than the corresponding alternatives that include solely a prime.
- Decision Alternative B is dominant over Decision Alternative C in all decision criteria and Decision Alternative J is dominant over Decision Alternative K in all decision criteria. Based on the findings, *Decision Alternatives C and K can be eliminated from final consideration.*

	Self	Self Now	Self Future	Self Future	Self Future	Self Future
			Alpha Inc.	Alpha Inc.	Charlie Inc.	Charlie Inc.
	Prime					
	Sub			Delta Inc.		Delta Inc.
	Decision Alternative	A	B	C	J	K
	Cost	\$ 17.5 (M)	\$ 10.0 (M)	\$ 10.0 (M)	\$ 14.0 (M)	\$ 14.0 (M)
	Aggregated Total Value Score	0.53	0.65	0.60	0.60	0.55
			+	+	+	+
33%	Aggregated Total Business Trust Score	0.91	0.93	0.85	0.77	0.74
			+	-	-	-
33%	Aggregated Total Security Maturity Score	0.65	0.56	0.51	0.81	0.67
			-	-	+	-
33%	Aggregated Total Financial Cost Score	0.03	0.44	0.44	0.22	0.22
			+	+	+	+
	Savings		\$ 7.5 (M)	\$ 7.5 (M)	\$ 3.5 (M)	\$ 3.5 (M)
	# of Negatives		1	2	1	2

Figure 55: Comparison of Decision Alternatives with and without Delta Inc. as a Sub

With the elimination of Decision Alternatives F and N in which Bravo Inc. and Delta Inc. are the primes, and Decision Alternatives C and K in which Delta Inc. is the sub, two *best* options remain, Decision Alternatives B and J (Figure 56, next page).

Equally Weighted		Alternative Providers				Decision Alternative Summary Scores		
Rank Order	Decision Alternative	Self	PRIME	SUB	Aggregated Total Value Score (100%)	Aggregated Total Business Trust Score (33%)	Aggregated Total Security Maturity Score (33%)	Aggregated Total Financial Cost Score (33%)
6	Decision Alt. A	Self Now	Current Operations		★ 0.53	0.91	0.65	0.03
1	Decision Alt. B	Self Future	Alpha Inc.	Top 2	0.65	0.93	0.56	0.44
3	Decision Alt. J	Self Future	Charlie Inc.		0.60	0.77	0.81	0.22

Figure 56: Best Two Decision Alternatives for Final Consideration

#### 5.4.4 Financial Cost Savings: Top Decision Alternatives Compared to Current Operations

In comparison with the Financial Cost of current operations, both Decision Alternatives B and J provide Financial Cost savings (Figure 57). Using Alpha Inc. as the prime (\$7.5 (M)) has a lower price tag than using Charlie Inc. as the prime (\$3.5 (M)); but, both options provide significant savings.

	Self	Self Now	Self Future	Self Future
	Prime	★ Current Operations	Alpha Inc.	Charlie Inc.
	Decision Alternative	A	B	J
	Financial Cost	\$ 17.5 (M)	\$ 10.0 (M)	\$ 14.0 (M)
	Total Value Score	★ 0.53	0.65	0.60
			+	+
33%	Financial Cost Utility Score	0.03	0.44	0.22
			+	+
	Financial Savings		\$ 7.5 (M)	\$ 3.5 (M)

Figure 57: Financial Cost Comparison of Best Two Options

From a traditional initial cost of implementation perspective, selecting Decision Alternative B over Decision Alternative J is the optimum choice. However, these lower operational costs also come with a cost in terms of Business Trust and Security Maturity. Choosing Decision Alternative B would decrease Security Maturity and choosing Decision Alternative J would decrease Business Trust.

Decision makers need to be informed about what is included with the cost savings of these two decision alternatives. A review of the Business Trust and Security Maturity Scores and the issues driving these scores is needed to gauge if the Total Cost of Ownership is worth the Financial Cost savings (Figure 58).

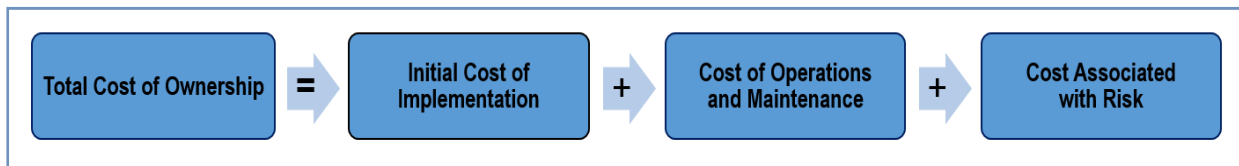


Figure 58: Total Cost of Ownership

### 5.4.5 Business Trust Analysis: Top Decision Alternatives Compared to Current Operations

Decision Alternative B scores in the High Business Trust Level and Decision Alternative J scores in the Moderate Business Trust Level. Decision Alternative B scores (0.93) slightly above current operations; whereas, Decision Alternative J score (0.77) decreases the overall Business Trust.

		Self Now	Self Future	Self Future
		★ Current Operations	Alpha Inc.	Charlie Inc.
			A	B
Decision Alternative Prime		\$ 17.5 (M)	\$ 10.0 (M)	\$ 14.0 (M)
Financial Cost		0.53	0.65	0.60
Total Value Score			+	+
33%	Business Trust Score	0.91	0.93	0.77
			+	-

Using the *Provider Business Category Display* to review the issues that are lowering the prime’s score in Decision Alternative J shows that Charlie Inc. received a score of Insufficient Evidence (0.0) for Category F “Non-U.S. Involvement and Control” (Figure 59). This is the only place in Business Trust or the Security Maturity Assessment that Charlie Inc. received an Insufficient Evidence score.

- *Note:* “Non-U.S. Involvement and Control” is an assessment area in the Business Trust model; it should also be considered a security concern. In fact, although “Non-U.S. Involvement and Control” is not specifically cited as a traditional cybersecurity technical concern, the importance of this component to supply chain risk management is a primary reason behind the inclusion of Business Trust in ONSAT.

From: *Provider Business Category Display*

Provider	Business Trust Score	Business Trust Basis Level	Business Trust Level ID	Business Trust Rank Order	A - SERVICE PROVIDER IDENTIFICATION	B - BUSINESS OWNER PROFILE	C - SERVICE PROVIDER PROFILE	D - MAJOR CHARACTERISTICS	E - MAJOR SPECIFIC REQUIREMENTS	F - NON-U.S. INVOLVEMENT AND CONTROL	G - BUSINESS RELATIONSHIPS, CLAIMS, JUDGEMENTS, AND CYBERSECURITY INCIDENTS	H - GENERAL REPUTATION AND HISTORICAL TRUST
Self Now	★ 0.92	High Trust Basis	4	3	0.95	0.95	0.95	0.83	0.91		0.95	0.85
Alpha Inc.	0.95	Very High Trust Basis	5	1	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
Charlie Inc.	0.62	Low Trust Basis	2	6	0.67	0.66	0.62	0.75	0.75	0.00	0.75	0.75

Figure 59: Business Trust Comparison of Best Two Options

**A Closer Look** is needed to determine if improving the scores for Categories A – C verification questions and resolving the Insufficient Evidence scores in Category F would make Charlie Inc. a more viable candidate in Business Trust; and thus improve the aggregated Business Trust of Decision J (see **A Closer Look**, next page).



**A CLOSER LOOK... Potential Improvement in Charlie Inc.'s Business Trust Score**

The *Provider Business Category Display* indicates that Charlie Inc. has a score of Insufficient Evidence (0.0) for Category F "Non-U.S. Involvement and Control".

- This is the only category in which Charlie Inc. has a response of Insufficient Evidence

Charlie Inc. also has a Level 1 Unverified Information rating for twelve out of the thirty verification questions in Business Trust Categories A – C. These scores do not follow the pattern of Level 5 Verified Information Charlie Inc. presents in the other eighteen verification questions.

- For example, it is improbable that Charlie Inc. has a score of Level 1 Unverified Information for Questions 1 – 3 (from *Example Business Assessment Tab*).

A		SERVICE PROVIDER IDENTIFICATION
V	1	Company/Business name
V	2	Company Primary Service Provider Location
V	3	Company Primary Service Provider Business Contact

Using the *Business Assessment Tab*:

- Modeling Charlie Inc.'s scoring with all verification questions in Business Trust Categories A – C at a Level 5 Verified Information *increases* Charlie Inc.'s Overall Business Trust Score from 0.62 to 0.73.
- Modeling Charlie Inc.'s scoring with all assessment questions in Business Trust Category F at a Level 3 Moderate Trust Level *increases* Charlie Inc.'s Business Trust Score from 0.73 to 0.83.

Charlie Inc.		Current Overall Business Trust Level and Score		Model Overall Business Trust Level and Score	
		Level 2 - Defined, Limited Scope 0.62		Level 2 - Defined, Limited Scope 0.73	
Category	Current Pattern for Categories A-C	Category Type	Model Pattern for Categories A-C Changed to Verified	and combined with	
A.	Level 1 - Unverified Information	V	Level 5 - Verified Information	Model Overall Business Trust Level and Score	
B.	Level 1 - Unverified Information	V	Level 5 - Verified Information		
C.	Level 1 - Unverified Information	V	Level 5 - Verified Information		
Category	Current Pattern for Categories D-H	Category Type	Model Pattern for Category F	Model Overall Business Trust Level and Score	
D.	Level 3 - Corporate Standard	A	Level 3 - Corporate Standard	Level 3 - Corporate Standard 0.83	
E.	Level 3 - Corporate Standard	A	Level 3 - Corporate Standard		
F.	Insufficient Evidence	A	Level 3 - Corporate Standard		
G.	Level 3 - Corporate Standard	A	Level 3 - Corporate Standard		
H.	Level 3 - Corporate Standard	A	Level 3 - Corporate Standard		

Modeling score values that align with Charlie Inc.'s score pattern in the remainder of the Business Assessment provides potential improvement in Charlie Inc.'s Business Trust Score from 0.62 Level 2 Low Trust to 0.81 Level 3 Moderate Trust. However, given that Business Trust is not a major deficiency in current operations (Decision Alternative A), this may not be the area that decision-makers want to emphasize. But if they do, the best choice of the two options is Decision Alternative B which slightly improves Business Trust over current operations and provides a financial savings of \$7.5 (M).

**5.4.6 Security Maturity Analysis: Top Decision Alternatives Compared to Current Operations**

Other than Financial Cost, Security Maturity is the greatest deficiency in current operations (Decision Alternative A). While cost savings is important, improving the security of the overall network services operations should be a primary concern of decision-makers. As such, Decision Alternative J might be the preferred choice since it improves security with a savings of \$3.5 (M) over current operations (below).

Self Prime	Self Now	Self Future	Self Future	
	★ Current Operations	Alpha Inc.	Charlie Inc.	
	Decision Alternative	A	B	J
	Financial Cost	\$ 17.5 (M)	\$ 10.0 (M)	\$ 14.0 (M)
	Total Value Score	★ 0.53	0.65	0.60
			+	+
33%	Security Maturity Score	0.65	0.56	0.81
		-	+	

Using the *Provider Security Category Display* to review the issues that are lowering the prime’s score in Decision Alternative B shows that Alpha Inc. has a score of 0.46 for all Security Maturity Categories. Alpha Inc.’s score is much lower than even the outsourcing organization’s score of 0.65 (Figure 60).

From: <i>Provider Security Category Display</i>		ONSAT Security Maturity Level Per Category																		
		Design Req. & Implement.	Data Flow	Asset & Audit	Information Assurance								Phys. Sec.	Per. Sec.	System Governance		Supply Chain			
Security Maturity Assessment Scoring Summary		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
Provider	Distribution of Question Answers	0.8	0.95	0.85	0.75	0.50	0.20	0.00												
	Not Applicable	Insufficient Evidence																		
Alpha Inc.	Level 5 - Corporate Optimization	20%																		
	Level 4 - Quantitatively Managed Standard	20%																		
	Level 3 - Corporate Standard	20%																		
	Level 2 - Defined, Limited Scope	20%																		
	Level 1 - Undefined, Undocumented	20%																		
	Rank Order	Insufficient Evidence																		
Provider	Overall Security Maturity Score	1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]																		
	Security Maturity Level	2) System Performance, Resiliency, and Security Architecture and Design Practices [System Design]																		
	Security Maturity Level ID	3) Communication Path, Data Flow, and Data Governance Policies and Practices [Data Governance]																		
	Rank Order	4) Asset Inventory and Audit Management Practices [Asset and Audit]																		
Self Now	★ 0.65	0.50	0.79	0.83	0.69	0.83	0.67	0.78	0.74	0.67	0.75	0.62	0.55	0.67	0.60	0.95	0.55	0.20	0.32	
Charlie Inc.	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	
Alpha Inc.	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	0.46	

Figure 60: Security Maturity Comparison of Best Two Options

In Section 5.1.2, **A Closer Look** at Alpha Inc.’s Insufficient Evidence responses (20%) determined that their resolution would not significantly raise Alpha Inc.’s overall Security Maturity Score. In fact, modeling substitution of the Insufficient Evidence values with Level 5 values did not raise Alpha Inc.’s overall Security Maturity Score out of Level 2 Defined, Limited Scope.

In particular, Decision Alternative B needs to improve its security scores in Security Maturity Categories related to Supply Chain: Category 17 – Asset Hardware / Software Integrity Protection Practices and Category 18 – Supplier Documentation and Vetting Policy and Practices. Both Alpha Inc. and the outsourcing organization scored very low in these two categories.

The outsourcing organization did improve its security posture as indicated in the comparison between Self Past and Self Now in the “Distribution of Question Answers” portion of the *Provider Security Display* Tab discussed in Section 5.1.2 (Figure 61).

- Trend analysis of Self Past and Self Now shows that the distribution of responses *increased* in Levels 2 and 3 and *decreased* in Level 5 and Insufficient Evidence.
- The decrease in Insufficient Evidence corresponds to the increase in Level 3 and improvement in Category 10 – Maintenance and Repairs Practices.
- The decrease in Level 5 corresponds to the increase in Level 2 and worsening in Category 1 – Mission and Security Requirements, Roles, Responsibilities, and Policies. These are two examples of the outsourcing organization’s effort in self-assessment.

From Provider Security Display		Distribution of Question Answers						
Security Maturity Assessment Scoring		0.6	0.95	0.85	0.75	0.50	0.20	0.00
Provider	Overall Security Maturity Score	Not Applicable	Level 5 - Corporate Optimization	Level 4 - Quantitatively Managed	Level 3 - Corporate Standard	Level 2 - Defined, Limited Scope	Level 1 - Undefined, Undocumented	Insufficient Evidence
Self Past	0.64	0%	18%	13%	26%	29%	9%	6%
			★	◆	★	★	◆	★
Self Now	0.65		11%	13%	32%	34%	9%	0%

Figure 61: Security Posture Improvement for Self Now

As the prime component of Decision Alternative B, Alpha Inc.’s very low Security Maturity Score when partnered with Self Now’s low Security Maturity Score presents a challenge to decision makers. While Decision Alternative J provides less financial savings than Decision Alternative B, Decision Alternative J is the **only** alternative that addresses **both** Financial Cost and Security Maturity deficiencies.

#### 5.4.7 Changing Decision Criteria Weights

As previously mentioned, another feature ONSAT provides is the ability for analysts and decision-makers to change the default weights of the three decision criteria (Business Trust, Security Maturity, and Financial Cost) from their equal weight (33.33%) values to new weights that reflect the relative needs of the organization. This is done in the *Decision Criteria – Weight Def* Tab. Relative to Business Trust, Security Maturity is a greater deficiency in current operations. Weighting Security Maturity greater than both Business Trust and Financial Cost is an opportunity to align a provider’s strengths against the outsourcing organization’s gaps to identify potential improvement in existing alternatives (Figure 62).

Lookup ID	Decision Criteria	Units of Measure	Criteria Importance Weight % Importance to Decision (Full Scale) User Defined	Criteria Importance Weight % Importance to Decision (Full Scale) Default Values (Equal Weight)	Used Swing Weight % Importance to Decision Among Actual Alternatives Calculated Value
			30%	33%	30%
User Defined	Business Trust	Continuous Trust Level Value (0 to 1)	30%	33%	30%
	Security Maturity	Continuous Security Maturity Value (0 to 1)	45%	33%	45%
	Financial Cost	U.S. Dollars in Millions (\$M)	25%	33%	25%
			100%	100%	100%

Figure 62: Decision Criteria – Weight Def. Tab with Revised Weights



Of the top seven decision alternatives, Decision Alternatives A, J, and K have increased Aggregated Total Value Score; whereas, scores for Decision Alternatives B, C, N, and F stayed the same. Decision Alternative A's increased Aggregated Total Value Score reflects the lower weight on Financial Cost and highlights that the outsourcing organization, with the exception of Charlie Inc., has a higher individual Security Maturity Score than the other providers. Using the revised decision criteria weights of Business Trust 30%, Security Maturity 45%, and Financial Cost 25%, the Aggregated Total Value Scores for the same assessment data shift to favor the decision alternatives with higher security maturity (Figure 63).

	Self			Self Now	Self Future	Self Future	Self Future	Self Future	Self Future	Self Future
	Prime				Alpha Inc.	Alpha Inc.	Charlie Inc.		Charlie Inc.	Bravo Inc.
	Sub					Delta Inc.		Delta Inc.	Delta Inc.	
	Decision Alternative			A	B	C	J	N	K	F
	Financial Cost			\$ 17.5 (M)	\$ 10.0 (M)	\$ 10.0 (M)	\$ 14.0 (M)	\$ 11.5 (M)	\$ 14.0 (M)	\$ 12.0 (M)
Aggregated Total Value Score	Weighted Equally									
	33%	33%	33%	0.53	0.65	0.60	0.60	0.57	0.55	0.53
	Weighted to Balance Security Gaps			★	◊	◊	★	◊	★	◊
	30%	45%	25%	★ 0.57	0.65	0.60	0.65	0.57	0.58	0.53
Aggregated Total Business Trust Score 30%				0.91	0.93	0.85	0.77	0.80	0.74	0.82
Aggregated Total Security Maturity Score 45%				0.65	0.56	0.51	0.81	0.53	0.67	0.43
Aggregated Total Financial Cost Score 25%				0.03	0.44	0.44	0.22	0.36	0.22	0.33
Cost Savings					\$ 7.5 (M)	\$ 7.5 (M)	\$ 3.5 (M)	\$ 6.0 (M)	\$ 3.5 (M)	\$ 5.5 (M)

Figure 63: Shift in Aggregated Total Value Scores based on Revised Weighting

The top two choices, Decision Alternative B and Decision Alternative J now have the same Aggregated Total Value Score (0.65) while the underlying individual assessment scores remain the same (Figure 64).

Using varied weights for decision criteria to balance the strengths and gaps of the outsourcing organization supports analysis and enables better risk management and a more secure supply chain.

	Self			Self Now	Self Future	Self Future
	Prime				Alpha Inc.	Charlie Inc.
	Sub					
	Decision Alternative			A	B	J
	Financial Cost			\$ 17.5 (M)	\$ 10.0 (M)	\$ 14.0 (M)
Aggregated Total Value Score	Weighted Equally					
	33%	33%	33%	0.53	0.65	0.60
	Weighted to Balance Security Gaps			★	◊	★
	30%	45%	25%	★ 0.57	0.65	0.65
Aggregated Total Business Trust Score 30%				0.91	0.93	0.77
Aggregated Total Security Maturity Score 45%				0.65	0.56	0.81
Aggregated Total Financial Cost Score 25%				0.03	0.44	0.22
Cost Savings					\$ 7.5 (M)	\$ 3.5 (M)

Figure 64: Comparison of Top Two Options with Revised Weighting

The greater weighting of Security Maturity is also reflected in the reordered ranking of Decision Alternatives in the Total Value Composite Chart (Figure 65). With the revised weighting, Decision



Alternative J is ranked as the best option and Decision Alternative B is now the second best option. Decision Alternative A, the option to not outsource, has moved up in rank order from number 6 to number 5. The information gleaned from decision analysis in Section 5.4 is used in Section 6 to provide findings and present recommendations to decision makers.

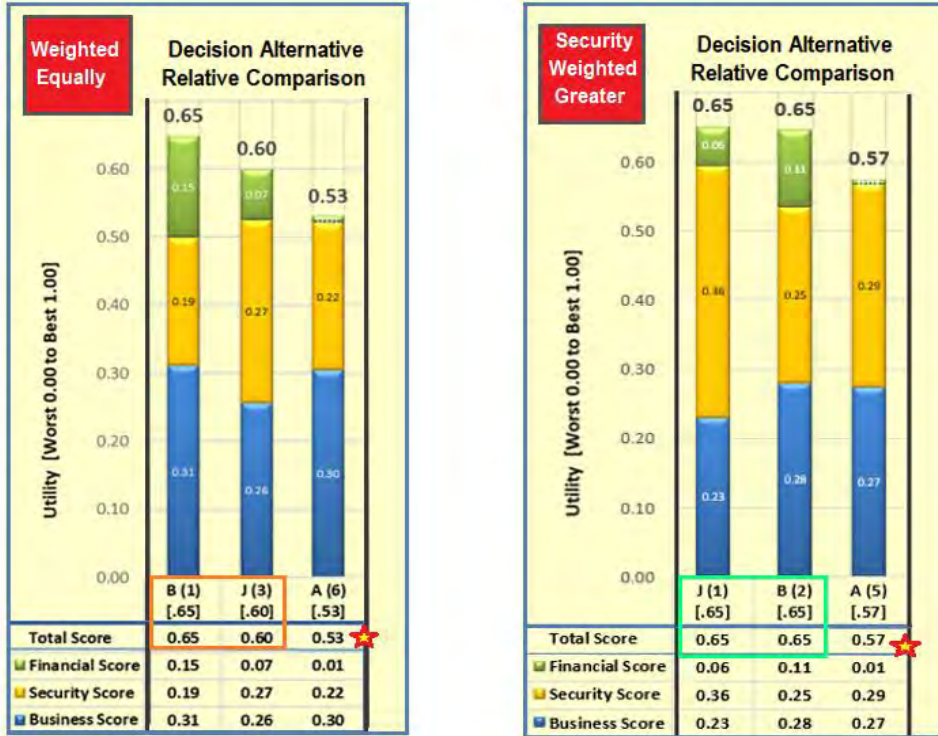


Figure 65: Top Two Decision Alternatives Ranking- Default and Revised Weighting

## 6.0 Step 6: Present Findings and Provide Recommendations



The primary purpose of conducting outsourcing assessments and analyzing the results is to assist decision makers in making better-informed decisions based on the best available evidence. The displays and content in Section 5 are designed to help users:

- Gain a better understanding of the available data and display format,
- Appreciate the impact of characteristics of individual providers on aggregated decision alternative scores, and
- Compare and contrast decision alternatives.

### 6.1 Preparing the Presentation to Decision Makers

As an outcome of the assessment process, the CIO, the assessment team, or other internal representatives prepare findings and recommendations for presentation to the decision-makers.

Presentation content and format is heavily dependent upon the individual decision-makers and the internal decision processes. Section 6.1 reviews the task assigned to the assessment team, the key objectives, and an overview of the decision alternatives assessed. The remainder of Section 6 is structured as briefing slides with summarized and numbered findings from analysis in Section 5 as well as recommendations for decision makers.

**Task:** Review proposals from multiple primes (and their subs) to provide corporate cloud data storage services of U.S. classified information in support of our organization’s mission / business line. Present the findings and provide recommendations to the executive board.

- As part of this task, conduct an assessment using ONSAT and summarize the status of Business Trust, Security Maturity, and Financial Cost Utility of each alternative starting with the individual providers comprising the alternatives.
- Additionally, conduct the same assessment of our organization.
- Compare findings at the Overall Assessment (Total Value), Business Trust, Security Maturity, and Financial Cost Utility levels to support recommendations to the executive board.

**Key objectives by the outsourcing organization:**

- Reduce Financial Costs of Operating Network Services
- Improve the Security Maturity Posture of Network Services
- Improve the Business Trust Posture of Network Services Providers
- Leverage Partnerships with Providers to Augment the Organization’s Focus on Continuous Improvement

**Decision Alternatives Explored:**

- Assessed Fifteen Decision Alternatives comprised of combinations of eight individual providers in roles of self, prime, or sub:
  - Self Now – current operations
  - Self Future –future internal operations performed under an outsourcing arrangement
  - Alpha Inc. – a prime
  - Bravo Inc. – a prime
  - Charlie Inc. – a prime
  - Delta Inc. – a prime and a sub
  - Echo Inc. – a prime and a sub
  - Foxtrot Inc. – a prime and a sub

## 6.2 Summary of Findings

### 6.2.1 Findings about Current Internally Provided Network Services

A quick synopsis of the organization’s self-assessment using ONSAT:

<b>Current Operating Costs</b>	<b>\$17.5 (M)</b>	<b>Highest Acceptable Cost</b>	<b>\$14.0 (M)</b>
<b>Alternative Rank Order</b>	<b>6th</b>		
	<i>Score</i>	<i>Level Description</i>	<i>Method for Determination</i>
<b>Overall Assessment</b>	<b>0.53</b>	<b>Unsatisfactory Alternative</b>	<b>Weighted Average</b>
<b>Overall Business Trust</b>	<b>0.91</b>	<b>High Trust Level</b>	<b>Questionnaire Assessment</b>
<b>Overall Security Maturity</b>	<b>0.65</b>	<b>Low Security Maturity</b>	<b>Questionnaire Assessment</b>
<b>Financial Cost Utility</b>	<b>0.03</b>	<b>Extremely Low Utility</b>	<b>Ranking of Alternatives</b>

## 6.2.2 Findings about Outsourcing Alternatives

### 6.2.2.1 Comparison of Decision Alternatives Overall Assessment Scores

Decision Alternatives are ranked based on their Overall Assessment Scores. Overall Assessment Score for each decision alternative is the Aggregated Total Value Score (100%) comprised of the Aggregated Total Scores for each of the criteria: Business Trust, Security Maturity, and Financial Cost Utility. The default weight assigned to each of the three criteria is 33% (equally weighted).

**Finding 1:** Comparison of the Overall Assessment Scores<sup>36</sup> of the initial set of decision alternatives identifies eight alternatives that can be eliminated from consideration.

Overall Assessment Scores of the Decision Alternatives Using Current Operations as a Baseline																																																																					
<p><b>Initial Set of 15 Decision Alternatives Compared to Decision Alternative A (Current Operations):</b></p> <ul style="list-style-type: none"> <li>8 alternatives have a lower Overall Assessment Score than Current Operations.</li> <li>All 8 Reduce Financial Cost, but do <b>not</b> improve either Security Maturity or Business Trust.</li> <li>All 8 eliminated from further analysis as there are other viable alternatives that Reduce Financial Cost <b>AND</b> improve either Security Maturity or Business Trust.</li> </ul>			<p><b>Scores of Eight Lowest-Ranked Alternatives</b></p> <table border="1"> <thead> <tr> <th>Rank</th> <th>Alternative</th> <th>Overall Assessment</th> <th>Business Trust</th> <th>Security Maturity</th> <th>Financial Cost Utility</th> <th>Financial Cost</th> </tr> </thead> <tbody> <tr> <td>8</td> <td>G</td> <td>0.51</td> <td>0.78</td> <td>0.42</td> <td>0.33</td> <td>\$ 12.0 (M)</td> </tr> <tr> <td>9</td> <td>D</td> <td>0.51</td> <td>0.71</td> <td>0.38</td> <td>0.44</td> <td>\$ 10.0 (M)</td> </tr> <tr> <td>10</td> <td>E</td> <td>0.50</td> <td>0.62</td> <td>0.43</td> <td>0.44</td> <td>\$ 10.0 (M)</td> </tr> <tr> <td>11</td> <td>L</td> <td>0.45</td> <td>0.60</td> <td>0.54</td> <td>0.22</td> <td>\$ 14.0 (M)</td> </tr> <tr> <td>12</td> <td>O</td> <td>0.45</td> <td>0.60</td> <td>0.33</td> <td>0.42</td> <td>\$ 10.5 (M)</td> </tr> <tr> <td>13</td> <td>M</td> <td>0.44</td> <td>0.51</td> <td>0.59</td> <td>0.22</td> <td>\$ 14.0 (M)</td> </tr> <tr> <td>14</td> <td>H</td> <td>0.42</td> <td>0.64</td> <td>0.29</td> <td>0.33</td> <td>\$ 12.0 (M)</td> </tr> <tr> <td>15</td> <td>I</td> <td>0.41</td> <td>0.55</td> <td>0.34</td> <td>0.33</td> <td>\$ 12.0 (M)</td> </tr> </tbody> </table>				Rank	Alternative	Overall Assessment	Business Trust	Security Maturity	Financial Cost Utility	Financial Cost	8	G	0.51	0.78	0.42	0.33	\$ 12.0 (M)	9	D	0.51	0.71	0.38	0.44	\$ 10.0 (M)	10	E	0.50	0.62	0.43	0.44	\$ 10.0 (M)	11	L	0.45	0.60	0.54	0.22	\$ 14.0 (M)	12	O	0.45	0.60	0.33	0.42	\$ 10.5 (M)	13	M	0.44	0.51	0.59	0.22	\$ 14.0 (M)	14	H	0.42	0.64	0.29	0.33	\$ 12.0 (M)	15	I	0.41	0.55	0.34	0.33	\$ 12.0 (M)
Rank	Alternative	Overall Assessment	Business Trust	Security Maturity	Financial Cost Utility	Financial Cost																																																															
8	G	0.51	0.78	0.42	0.33	\$ 12.0 (M)																																																															
9	D	0.51	0.71	0.38	0.44	\$ 10.0 (M)																																																															
10	E	0.50	0.62	0.43	0.44	\$ 10.0 (M)																																																															
11	L	0.45	0.60	0.54	0.22	\$ 14.0 (M)																																																															
12	O	0.45	0.60	0.33	0.42	\$ 10.5 (M)																																																															
13	M	0.44	0.51	0.59	0.22	\$ 14.0 (M)																																																															
14	H	0.42	0.64	0.29	0.33	\$ 12.0 (M)																																																															
15	I	0.41	0.55	0.34	0.33	\$ 12.0 (M)																																																															

All six of the remaining alternatives overall score as well or better than Current Operations; and therefore, there is benefit to reviewing these outsourcing alternatives to see whether or not the benefits are cost effective at the decision level.

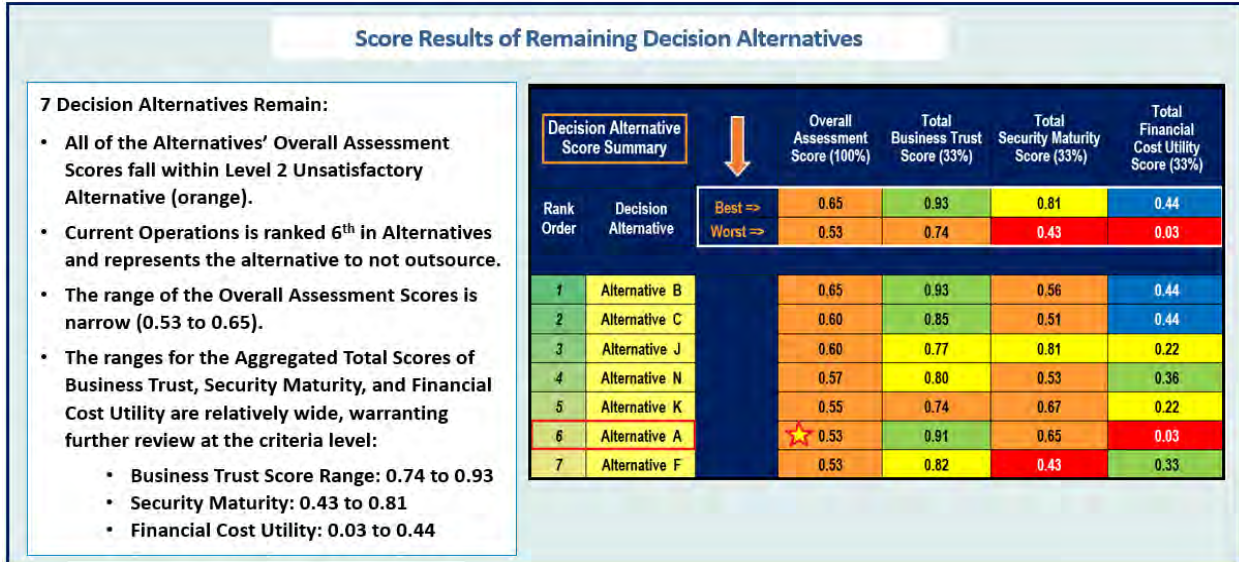
### 6.2.2.2 Comparison of Remaining Decision Alternatives Scores

**Finding 2:** Comparison of the remaining decision alternatives scores shows that based on overall scores, the three best alternatives are Alternatives B, C, and J. All alternatives are rated as Level 2, Unsatisfactory Alternative; however, the wide range of scores in Business Trust, Security Maturity and Financial Cost Utility indicates that the Overall Assessment Score can mask key information (see slide, next page).

*This is Blank Space*

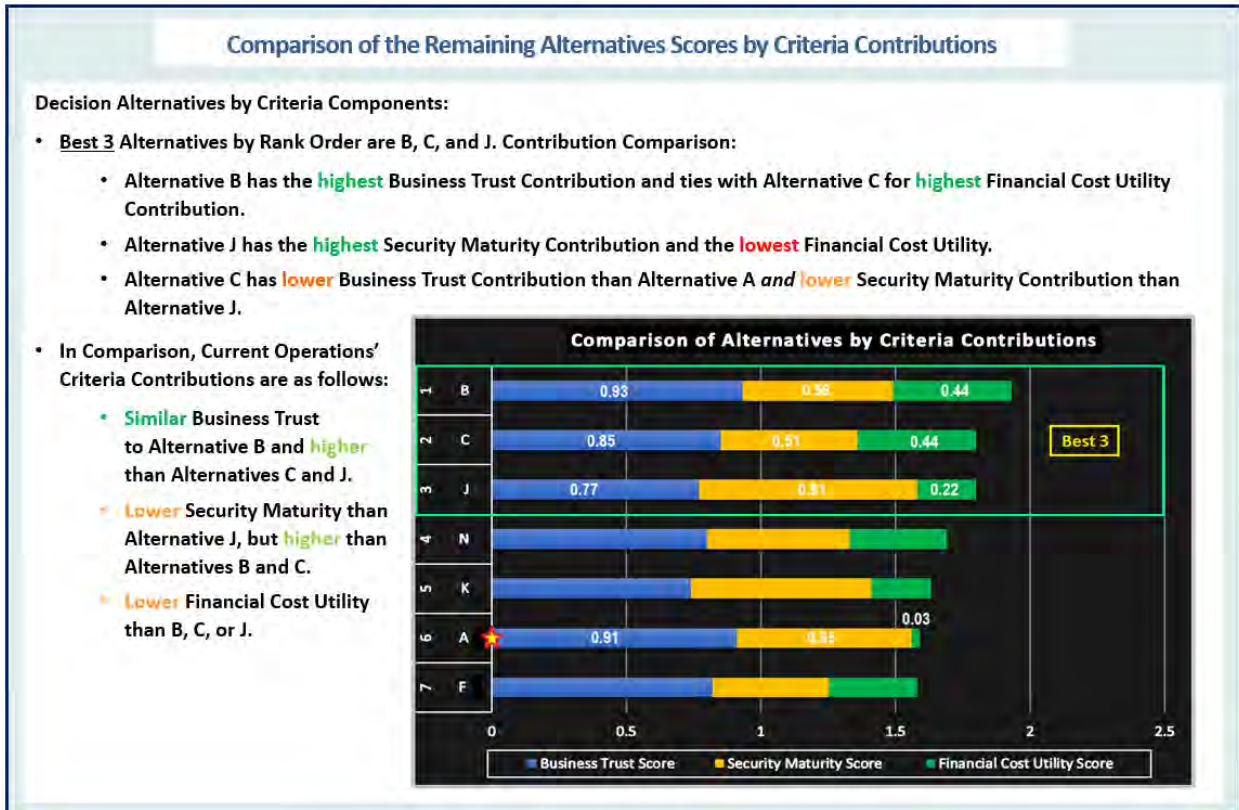
<sup>36</sup> Overall Assessment Score and Decision Alternative Total Value Score and Aggregated Total Value Score are interchangeable for this briefing.





### 6.2.2.3 Comparison of the Remaining Alternatives Scores by Criteria Contributions

**Finding 3:** Comparison of the remaining decision alternatives by criteria contribution shows that Alternative B has the highest contributions in Business Trust and Alternative J has the highest contribution in Security Maturity. Alternative C ties with the Alternative B for the highest Financial Cost Utility *but* has a lower contribution in Business trust and Security Maturity than Current Operations, indicating that examination at the criteria contribution level is warranted.

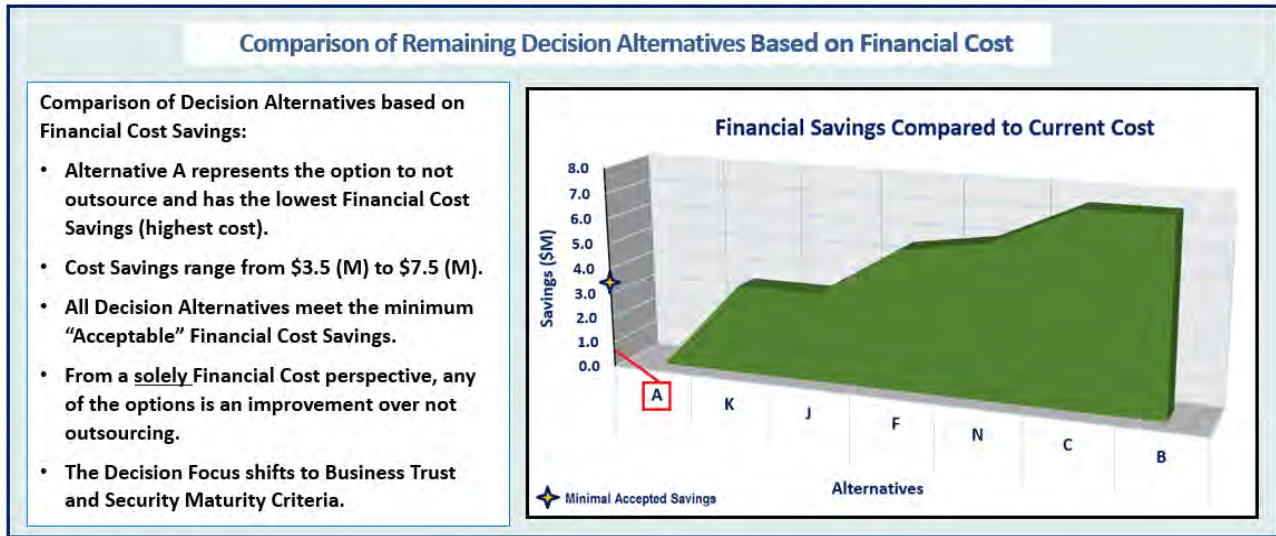




### 6.2.2.3.1 Comparison of Remaining Decision Alternatives: Financial Cost

The Financial Cost Utility Value Score<sup>37</sup> enables comparisons with Business Trust and Security Maturity Scores. When discussed individually, Financial Cost (\$) or Financial Cost Savings (\$ or %) can be used.

**Finding 4:** Decision Alternative A represents the option to not outsource and has the lowest Financial Cost Savings (highest Financial Cost). All the other cost alternatives are “acceptable” and a significant improvement compared to the current operations cost of internally providing the network services.



### 6.2.2.3.2 Comparison of Remaining Decision Alternatives: Business Trust and Security Maturity

With all cost alternatives deemed “acceptable”, the decision focus shifts to selecting the decision alternative with the correct balance of Business Trust and Security Maturity; the correct balance differs based on organization and scenario.

The remaining decision alternatives (at right) include Self Now, the option to not outsource, along with six alternatives.

All six alternatives are comprised of Self Future and a prime or Self Future, a prime, and a sub. Self Future represents the internal operations performed under an outsourcing arrangement.

Decision Alternative	Self	Prime	Sub (Sub As Prime)
A	Self Now		
B	Self Future	Alpha Inc.	
C	Self Future	Alpha Inc.	Delta Inc.
J	Self Future	Charlie Inc.	
K	Self Future	Charlie Inc.	Delta Inc.
N	Self Future		Delta Inc.
F	Self Future	Bravo Inc.	

**Finding 5:** Alternative B has the highest Business Trust and Alternative J has the highest Security Maturity (see slide, next page).

**Finding 6:** Alternatives comprised of a prime and a sub have a lower Business Trust Score or Security Maturity than the associated alternative comprised solely of the prime (see slide, next page).

- Alternative C has a lower Business Trust Score than Alternative B (Table 1 in the slide below).

<sup>37</sup> Refer to [Section 2.1.4 Financial Assessment and Associated Scale](#) for details on the Financial Cost Utility Value.

- Alternative K has a lower Security Maturity Score than Alternative J (Table 1 in the slide below).

**Finding 7:** Alternatives F and K have both a lower Business Trust and Security Maturity Score than Current Operations and are not viable options, regardless of Financial Cost.

**Comparison of Remaining Decision Alternatives in Business Trust and Security Maturity**

Comparisons of Remaining Decision Alternatives Based on Business Trust and Security Maturity:  
Scores for Current Operations indicates that Business Trust is an *area of strength* and Security Maturity is an *area of deficiency* for the outsourcing organization.

Compared to Current Operations:

- All alternatives are marked as **negatively** impacting (-) Business Trust, except for Alternative B (+).
- All alternatives are marked as **negatively** impacting (-) Security Maturity, except Alternative J (+).

Alternatives with **2 Negatives** are **eliminated** from Further Consideration:

- Alternatives (C and K) comprised of a prime and a sub score lower in Business Trust Score and/or Security Maturity than the associated Alternatives (B and K) comprised of solely the prime (Table 1).
- Alternatives N and F have lower Business Trust and Security Maturity Scores than Current Operations (Table 2).

Equal Weighting	Self Prime	Self Now	Self Future	Self Future	Self Future	Self Future
	Sub		Alpha Inc.	Alpha Inc.	Charlie Inc.	Charlie Inc.
Decision Alternative	★ A		B	C	J	K
Rank Order	6		1	2	3	5
Cost	\$ 17.5 (M)		\$ 10.0 (M)	\$ 10.0 (M)	\$ 14.0 (M)	\$ 14.0 (M)
33%	Aggregated Total Business Trust Score	0.91 + or -	0.93 → 0.95 +	0.95 -	0.77 → 0.74 -	0.74 -
33%	Aggregated Total Security Maturity Score	0.65 + or -	0.56 → 0.51 -	0.51 -	0.81 → 0.67 +	0.67 -
Total # of Negatives (-)			1	2	1	2

Equal Weighting	Self Prime	Self Now	Self Future	Self Future	Self Future	Self Future
	Sub		Alpha Inc.	Charlie Inc.	Delta Inc.	Bravo Inc.
Decision Alternative	★ A		B	J	N	F
Rank Order	6		1	3	4	7
Cost	\$ 17.5 (M)		\$ 10.0 (M)	\$ 14.0 (M)	\$ 11.5 (M)	\$ 12.0 (M)
33%	Aggregated Total Business Trust Score	0.91 + or -	0.93 +	0.77 -	0.80 -	0.82 -
33%	Aggregated Total Security Maturity Score	0.65 + or -	0.56 -	0.81 +	0.53 -	0.43 -
Total # of Negatives (-)			1	1	2	2

### 6.2.3 Comparison of Two Best Options with Redefined Weights

With elimination of the four decision alternatives, Alternative B and Alternative J are the top two options remaining. Other than Financial Cost, Security Maturity is the *greatest deficiency* in current operations.

- As the prime component of Decision Alternative B, Alpha Inc.’s very low Security Maturity when partnered with the outsourcing organization’s low Security Maturity presents a challenge to decision makers.
- While Alternative J provides less financial savings than Alternative B, Charlie Inc. as the prime component of Alternative J addresses **both** Financial Cost and Security Maturity deficiencies.

**Finding 8:** Using the revised decision criteria weights of Business Trust 30%, Security Maturity 45%, and Financial Cost 25%, Alternative J is now ranked the best option, with Alternative B ranked second, and Current Operations as fifth (see slide on next page).


*This is Blank Space*

### Comparison of Two Best Decision Alternatives Based on Redefined Weights

**Comparisons of Two Best Options Based on Redefined Weights:**

**Emphasizing Security Maturity by Weighting it more than Business Trust and Financial Cost** →

Leverages Current Operations' **High Business Trust** to Partner with a Provider to Fill Critical **Security Maturity Gaps** and **Reduce Financial Cost**.



Decision Criteria	Units of Measure	Criteria Importance Weight % Importance to Decision (Full Scale) User Defined
Business Trust	Continuous Trust Level Value (0 to 1)	30%
Security Maturity	Continuous Security Maturity Value (0 to 1)	45%
Financial Cost	U.S. Dollars in Millions (\$M)	25%

The underlying individual assessment scores remain the same while the **Aggregated Total Value Scores** Shift to Favor the Alternative with higher Security Maturity.

- Alternative J and Alternative B now have the same Aggregated Total Value Score (0.65).
- Alternative J is now ranked #1, Alternative B is ranked #2, and Current Operations is now ranked #5.

	Self Prime			Self Now	Self Future	Self Future
	Charlie Inc.	Alpha Inc.	Charlie Inc.		Alpha Inc.	
Decision Alternative				5	1	2
Financial Cost				\$ 17.5 (M)	\$ 14.0 (M)	\$ 10.0 (M)
Weighted Equally						
Aggregated Total Value Score	33%	33%	33%	0.53	0.60	0.65
Weighted to Balance Security Gaps						
	30%	45%	25%	0.57	0.65	0.65
Aggregated Total Business Trust Score 30%				0.91	0.77	0.93
Aggregated Total Security Maturity Score 45%				0.65	0.81	0.56
Aggregated Total Financial Cost Score 25%				0.03	0.22	0.44
Cost Savings					\$ 3.5 (M)	\$ 7.5 (M)

### 6.3 Review of Self-Assessment to Inform Business Goals

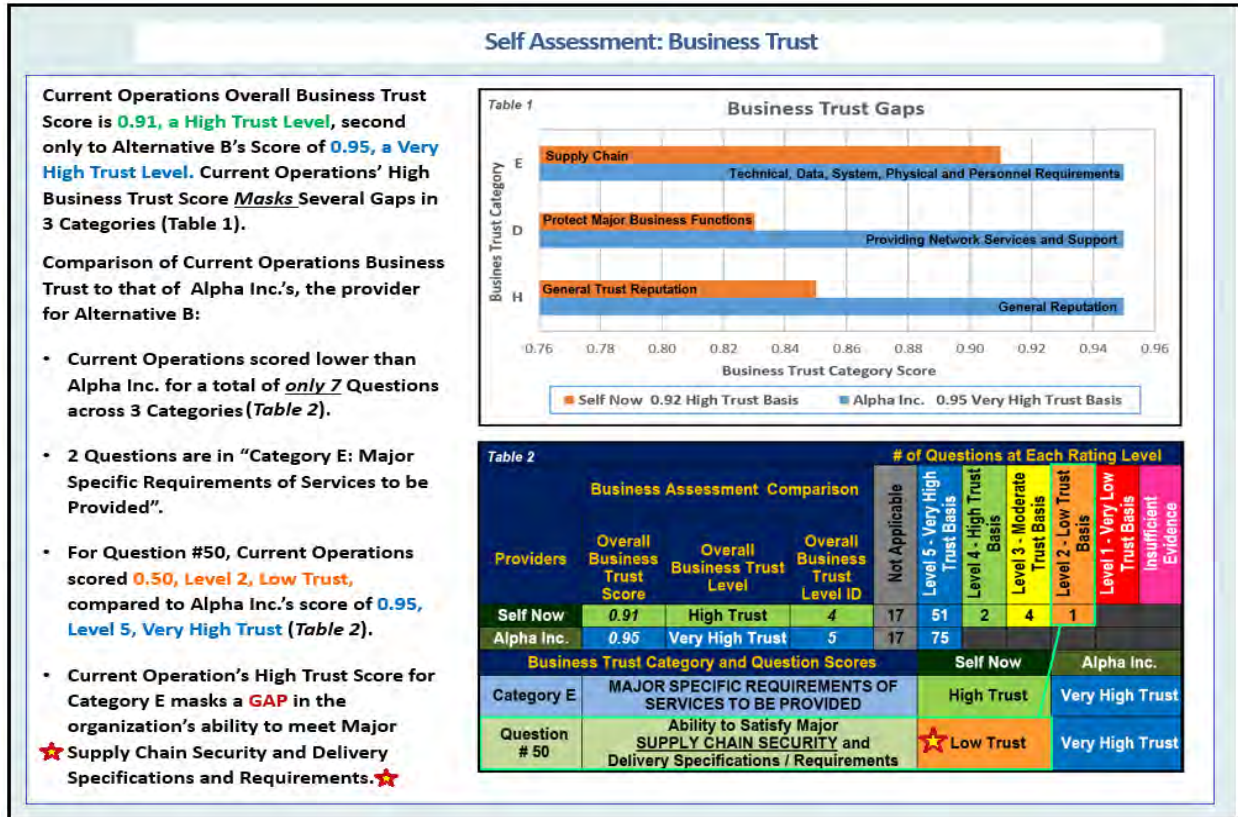
Briefing Decision Makers should include a review of the organization's most recent self-assessment and alignment of progress with business goals and concerns.

#### 6.3.1 Review of Self-Assessment: Business Trust

**Finding 9:** Current Operations' Self-Assessment revealed that the organization's high Business Trust Score masks deficiencies in several areas including a critical gap in Supply Chain (see slide, next page).

*This is Blank Space*





### 6.3.2 Review of Self-Assessment: Security Maturity

**Finding 10:** Current Operations' Self-Assessment highlighted a critical gap in Supply Chain Security and poor performance in four areas including Personnel Training (see slide, next page).

**Finding 11:** Current Operations' Self-Assessment identified that four areas met the performance goal of Corporate Standard Level 3, and the Performance Management Practices area rated at the highest score of Level 5, Corporate Optimization (see slide, next page).

**Finding 12:** Current Operations' Self-Assessment identified 7 areas in which solid performance was masked by smaller deficiencies (see slide, next page).

*This is Blank Space*



### Self Assessment: Security Maturity

Current Operations has an Overall Security Maturity Score of **0.65**, a **Low Level 2 Limited Scope** rating.

Comparison of Current Operations to Charlie Inc., the provider for Alternative J:

- Alternative J is ranked 1<sup>st</sup> with a of **0.95**, a **Very High, Corporate Optimization**; 3 levels higher than Current Operations.

Self Assessment:

- Progress:** Performance Management Practices as Level 5 and Corporate Standard Level 3 for 4 areas.
- Concerns:** Poor Performance in 4 areas including Personnel Training and Critical Gap in 2 areas of Supply Chain
- Additional Focus:** Solid Performance in 7 areas masked by smaller gaps.

Continuous Security Improvement Progress	Design Req. & Implement.	Data Flow	Asset & Audit	Information Assurance								Phys. Sec.	Per. Sec.	System Governance	Supply Chain			
<b>Key</b>	1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]	2) System Performance, Resiliency, and Security Architecture and Design Practices [System Design]	3) Communication Path, Data Flow, and Data Governance Policies and Practices [Data Governance]	4) Asset Inventory and Audit Management Practices [Asset and Audit]	5) Authentication and Access Control Practices [Info. Sys. Security]	6) Network Segmentation Practices [Info. Sys. Security]	7) Data Confidentiality, Integrity and Availability Protection Practices [Info. ]	8) Vulnerability and Resilience Management Practices [Info. ]	9) Configuration Management Practices [Info. ]	10) System Maintenance and Repairs Practices [Info. ]	11) Incident Detection and Response [Info. ]	12) Consequence / Impact Recovery Policies and Practices [Info. ]	13) Physical / Facilities Security Policies and Practices [Physical Security]	14) Personnel Security Policies, Awareness, and Training [Personnel Security]	15) Performance Management Practices [System Governance]	16) Governance, Risk, and Compliance (GRC) Management Practices [System Governance]	17) Asset HWSW Integrity Protection Practices [Supply Chain]	18) Supplier Documentation and Vetting Policy and Practices [Supply Chain]
Current Status	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Self Now	0.50	0.79	0.83	0.69	0.83	0.67	0.78	0.74	0.67	0.75	0.62	0.55	0.67	0.60	0.95	0.55	0.20	0.32

### 6.3.3 Business Goals Informed by Self-Assessment

#### Business Goals and Focus Areas Informed by Self Assessment

**Business Goals Informed by Self Assessment:**

- Focus on Multiple Gaps in Security is Necessary to Reach Longer Term Goal of Continuous Security Maturity.
- Mitigation of Deficiencies in Supply Chain and Personnel Security and Training *Benefits* Both Continuous Security Maturity and Business Trust.

#### Goals and Focus Areas Informed by Self Assessment

<p><b>Longer Term</b></p> <p><i>Continuous Security Maturity</i></p> <ul style="list-style-type: none"> <li>- Supply Chain</li> <li>- Personnel Security and Training</li> <li>- Design: Mission and Security Requirements, Roles, and Responsibilities</li> <li>- Information Assurance: Impact Recovery</li> <li>- System Governance: Governance, Risk, and Compliance</li> </ul>	<p><b>Short Term</b></p> <p><i>Mitigate Gaps in Business Trust</i></p> <ul style="list-style-type: none"> <li>- Supply Chain</li> <li>- Evidence and Verification Training</li> <li>- Personnel Security and Training</li> <li>- Compliance</li> <li>- Protection Policies and Practices</li> </ul>	<p><b>Near Term</b></p> <p><i>Outsource Network Services</i></p> <ul style="list-style-type: none"> <li>- Partner with Cloud Service Provider</li> <li>- Leverage Cost Savings to Fund Long and Short Term Objectives</li> </ul>
---	---	--

## 6.4 Decision Recommendations: Option 1 and Option 2

### Decision Recommendations: Option 1 and Option 2

**"Best Option"** for the Organization is a Trade-Off: *Higher Financial Cost of Option 1 vs. High Security Risk Cost of Option 2*

**Recommendation:** Based on Current Operations' High Business Trust, Select the Provider with Strong Security Maturity to Compensate for Security Deficiencies and Critical Supply Chain Gaps.

Option 1: Alternative J	Option 2: Alternative B
<p><b>Pros:</b></p> <ul style="list-style-type: none"> <li>- Provides Significant Improvement in Security Maturity                             <ul style="list-style-type: none"> <li>- Covers Current Operations Gaps in <u>ALL</u> Categories</li> </ul> </li> <li>- Provides Financial Savings of \$ 3.5 (M) over Current Cost</li> </ul> <p><b>Cons:</b></p> <ul style="list-style-type: none"> <li>- Moderately Decreases Business Trust</li> </ul> <p><b>Conditions:</b></p> <ul style="list-style-type: none"> <li>- Charlie Inc. score in Business Trust Category F: Non-U.S. Involvement and Control is "Insufficient Evidence".</li> <li>- Modeling Substitution of Level 3 Corporate Standard Values for the "Insufficient Evidence" response improves the Business Trust Score.</li> <li>- If Charlie Inc. can provide or clarify evidence for Category F, then Alternative J is the "Best Option".</li> </ul>	<p><b>Pros:</b></p> <ul style="list-style-type: none"> <li>- Provides Slight Improvement in Business Trust                             <ul style="list-style-type: none"> <li>- Covers Current Operations Gaps in <u>3</u> Categories</li> </ul> </li> <li>- Provides Significant Financial Savings of \$ 7.5 (M) over Current Cost</li> </ul> <p><b>Cons:</b></p> <ul style="list-style-type: none"> <li>- Significantly Decreases Security Maturity                             <ul style="list-style-type: none"> <li>- Alpha Inc. the Provider for Alternative B, scored at a Low Security level across <u>ALL</u> 18 Security Categories.</li> </ul> </li> <li>- Mimics Current Operations skewed posture between Business Trust Security Maturity.</li> </ul> <p><b>Conditions:</b></p> <ul style="list-style-type: none"> <li>- If Option 1 is not viable, then the Additional Financial Savings afforded by Alternative B must be Focused on Improving Security Maturity, <i>especially</i> the Critical Gap in Supply Chain.</li> </ul>

*This is Blank Space*

## 7.0 References for Additional Reading

Analytic Approaches to Detect Insider Threats, December 2015, Carnegie Mellon University, Software Engineering Institute; retrieved from: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=451065>

An Approach to Assessing Vendors to Lower Potential Risk of Outsourced Network Services, The Open Group Guide (G197), March 2020, published by The Open Group; refer to: [www.opengroup.org/library/g197](http://www.opengroup.org/library/g197)

Carnegie Mellon University, Software Engineering Institute. Analytic Approaches to Detect Insider Threats. (2015, December 9). Retrieved May 16, 2020, from <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=451065>

Golafshani, N. Understanding Reliability and Validity in Qualitative Research. The Qualitative Report, 8(4), 597-606. (2003). Retrieved May 16, 2020, from <http://nsuworks.nova.edu/tqr/vol8/iss4/6>

NSA. (2020, January 22). Cybersecurity Mitigating Cloud Vulnerabilities. Retrieved May 16, 2020, from [https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES\\_20200121.PDF](https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF)

Wolford, B. (2019, February 22). Data Processing Agreement (Template). Retrieved May 16, 2020, from <https://gdpr.eu/data-processing-agreement/>

Wolford, B. (2019, February 13). Does the GDPR apply to companies outside of the EU? Retrieved May 16, 2020, from <https://gdpr.eu/companies-outside-of-europe/>

## 8.0 Glossary: Lexicon & Terminology

*In this user manual, terms are first and foremost defined for practical use of the tool and secondly by known industry standards as applicable to supply chain risk management.*

**Analysis of Alternatives** – an analytical comparison or evaluation of proposed approaches to meet an objective. An analysis of alternatives can be applied to anything – from a large military acquisition decision to a decision between two products. The formal or informal process involves identifying key decision factors, such as lifecycle operations, support, training, and sustainment costs, risk, effectiveness, and assessing each alternative with respect to these factors. An analysis of alternatives is an analytical comparison of the operational effectiveness, cost, and risks of proposed material solutions to gaps and shortfalls in operational capability. Such analyses document the rationale for identifying/recommending a preferred solution or solutions to the identified shortfall. Threat changes, deficiencies, obsolescence of existing systems, or advances in technology can trigger an analysis of alternatives. (NIST SP 800-160, Vol. 1)

**Asset** – anything that has value to the organization. (ISO 27001)

**Availability** – the property of being accessible and usable upon demand by an authorized entity. (ISO 27001)



**Body of Evidence** – the totality of evidence used to substantiate trust, trustworthiness, and risk relative to the system. (NIST SP 800-160, Vol. 1). The Oxford dictionary defines evidence as the “available body of facts or information indicating whether a belief or proposition is true or valid”<sup>38</sup>. See also **Evidence**

**Business Trust** – is a component to the risk management decision to outsource and corresponds to the total cost of ownership “care about” for the outsourcing organization. In the tool, business trust refers to the assessed degree of “Trust Basis”; refer to Section 2.1.3 for details on the Information Verification Scale (2.1.3.2) and the Information Trust Basis Scale (2.1.3.3)

**Confirmability** – in context of appraising evidence, the objectivity of the assessor and/or researcher i.e. the findings of a study are shaped by the respondents and not researcher bias, motivation, or interest<sup>39</sup>

**Credibility** – in context of appraising evidence, the confidence in the “veracity” of the findings i.e. answers, “How do you know that your findings are true and accurate?”<sup>40</sup>

**Critical infrastructure** – is defined in Executive Order 13626: Improving Critical Infrastructure Cybersecurity as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”<sup>41</sup>

**Confidentiality** – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (44 U.S.C. Sect 3542)

**Dependability** – in context of appraising evidence, the reliability of the assessment i.e., similar findings would be obtained if assessment repeated<sup>42</sup>

**Enterprise** – an organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects; acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. (CNSSI No. 4009)

**Evidence** – “take-it-to-the-bank, credible, documented, verified, validated versus asserted” information used to obtain assurance, substantiate trustworthiness, and assess risk // Grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood.

---

<sup>38</sup> <https://en.oxforddictionaries.com/definition/evidence>

<sup>39</sup> Barends, E., Rousseau, D.M., & Briner, R.B. (2014). *Evidence Based Management: The Basic Principles*. Amsterdam: Center for Evidence-based Management. <https://www.cebma.org/wp-content/uploads/Evidence-Based-Practice-The-Basic-Principles.pdf>

<sup>40</sup> Statistics Solutions. (n.d.). What is credibility in qualitative research and how do we establish it? [Blog post]. Retrieved from <https://www.statisticssolutions.com/what-is-credibility-in-qualitative-research-and-how-do-we-establish-it/>

<sup>41</sup> Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, 2013; retrieved from: <https://obamawhitehouse.archives.gov/the-pressoffice/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

<sup>42</sup> Statistics Solutions. (n.d.). What is credibility in qualitative research and how do we establish it? [Blog post]. Retrieved from <https://www.statisticssolutions.com/what-is-credibility-in-qualitative-research-and-how-do-we-establish-it/>



- Note 1: Evidence can be objective or subjective. Evidence is obtained through measurement, the results of analyses, experience, and the observation of behavior over time.
- Note 2: The security perspective places focus on credible evidence used to obtain assurance, substantiate trustworthiness, and assess risk. (NIST SP 800-160, Vol. 1)

**Financial Cost** – is a component to the risk management decision to outsource. In the tool, the Financial Cost corresponds to the "Utility Value of the Cost" to the outsourcing organization based on a user – defined budget and the available evidence entered by the assessor(s). The Cost Utility Value is comparable to the Business Trust and Security Maturity components. The Financial Cost is both a monetary descriptor and a utility value score; refer to Section 2.1.4 of this manual for details on the Financial Assessment Scale.

**Information and Communications Technology (ICT)** – the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information. [ISO/IEC 2382] (adapted)

**Information and Communications Technology (ICT) Sector** – in this manual, the ICT sector includes providers and integrators of information or communications hardware and software, and providers of information and/or communication services.

**Information and Communications Technology (ICT) Supply Chain** – (1) This system of networks includes organizations, people, processes, products, and services and the infrastructure supporting the system development life cycle, including research and development (R&D), design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement) of an organization's ICT products (i.e., hardware and software) and services. (2) The information and communications technology (ICT) supply chain is a complex, globally distributed system of interconnected networks that are logically long, with geographically diverse routes and multiple tiers of outsourcing. (NIST 800-161). Today's ICT supply chains have increased complexity, diversity, and scale.

**Information Security Management System (ISMS)** – is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. (ISO/IEC 27001)

**Insufficient Evidence** – information that does not meet the level of credible documentation that has been verified and validated in order to make an assessment to obtain assurance, substantiate trustworthiness, and assess risk. (See also Evidence)

**Integrity** – the property of safeguarding the accuracy and completeness of assets. (ISO 27001)

**Lifecycle** – Evolution of a system, product, service, project, or other human-made entity from conception through retirement. (ISO/IEC/IEEE 15288)

**Metrics** – tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

**Not Applicable** – does not apply to the outsourcing scenario or defined problem; and/or, organization or company is specifically restricted from engaging or operating within the parameters cited.

**Organization** – an entity of any size, complexity, or positioning within an organization structure (e.g., a federal agency or, as appropriate, any of its operational elements). (FIPS 200, Adapted)

**Outsourced Network Services** – a contract or other business relationship involving the acquisition of services to support the planning, design, implementation, operation, security, optimization, and life cycle support of an Information and Communications Technology (ICT) Infrastructure, including the core of the infrastructure, its end points, or anything in between. This can involve all or any portion of the described services.

For the ONSAT User Manual, examples of services explicitly included:

1. Network Transport Services,
2. Network-based Hosting Services,
3. Network-based Cloud Services,
4. Network-based DNS Services,
5. Network Service Provisioning,
6. Network Analysis & Performance Optimization,
7. Network Hardware/Software Monitoring & Management,
8. Specialized Network Software Development,
9. Network Traffic Flow Analysis & Reporting,
10. Network Component Installation & Repair,
11. Network-based Security Services, and
12. Mobile End-point Device management

Examples of services that are applicable when using ONSAT but were not explicitly included in the scope of tool design:

1. Timekeeping, Payroll Processing
2. Training, Professional Development
3. General H/R Services- hiring, performance management, health care, retirement, 401K, etc.
4. Internal Communications
5. External Communications
6. Customer Billing: PII Data for bill processing
7. Customer Care – Call Center, Help Desk, Issue Notification

**Outsourcing Organization** – for this manual, the organization that has made a decision to outsource some or all of its network management systems/services.

**Resilience** – the ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time span consistent with mission needs. (NIST SP 800-39)

**Risk** – the potential that a threat will exploit a vulnerability to cause harm or impact to an organization. // Also defined as: a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (CNSSI No. 4009)

**Risk Assessment** – the output generated from the risk assessment process

**Risk Assessment Process** – the overall process of risk analysis and risk evaluation. (ISO 27001)

**Risk Management** – process/activities to determine those risks with the greatest impact and greatest probability of occurring and assigning them a greater priority (prioritize addressing greatest impact and greatest probability of occurring first); thus, risk management is a method by which to focus mitigation efforts to meet risk tolerance. //Also defined as: coordinated activities to direct and control an organization with regard to risk. (ISO 27001) // The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. (CNSSI No. 4009)

**Risk Tolerance** – the level of risk an entity is willing to assume in order to achieve a potential desired result. (NISTIR 7298)

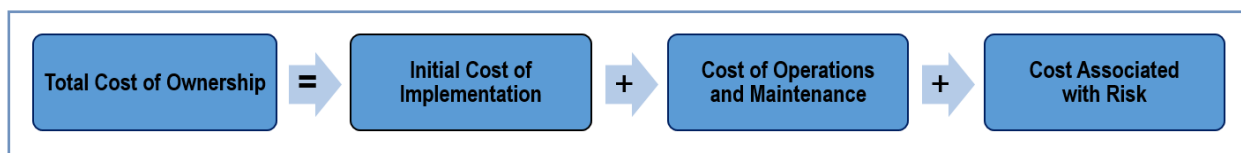
**Security Maturity** – is a component to the risk management decision to outsource and corresponds to a total cost of ownership “care about” for the outsourcing organization. In the tool, security maturity is the assessed level of “maturity of implemented security practices”; refer to Section 2.1.3.5 of this manual for details on the Security Maturity.

**Supply Chain** – linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and **services** and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. (NIST SP 800-53 Rev.4)

**Supply Chain Risk Management (SCRM)** – the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. (CNSSI No. 4009)

**Transferability** – in context of appraising evidence, the findings are applicable to other contexts e.g. similar situations / endeavors, and/or similar populations<sup>43</sup>

**Total cost of ownership** –the sum of the Initial Cost of Implementation, plus the Cost of Operations and Maintenance, plus the Cost Associated with Risk. The Total Cost of Ownership lasts for the lifecycle of an outsourcing decision.



**Weighted Average** – Sum of the values multiplied by their respective weights; the sum of the weights must equal 1.00 (see table, next page).

<sup>43</sup> Lincoln, YS. & Guba, EG. (1985). [Naturalistic Inquiry](http://www.qualres.org/HomeLinc-3684.html). Newbury Park, CA: Sage Publications. Retrieved from <http://www.qualres.org/HomeLinc-3684.html>

**Weighted Average = (EXCEL: Sum Product)**

$$(Weight_a * Value_a) + (Weight_b * Value_b) + (Weight_c * Value_c)$$

$$\sum_{i=a}^c (Weight_i) = 1.00$$

		a	b	c	Sum
Different	Weight	0.12	0.50	0.38	1.00
	Value	0.91	0.65	0.03	
	Result	0.11	0.33	0.01	0.45
Equal	Weight	0.33	0.33	0.33	1.00
	Value	0.91	0.65	0.03	
	Result	0.30	0.22	0.01	0.53

**Example when weights differ across assessment**

$$(0.12 * 0.91) + (0.50 * 0.65) + (0.38 * 0.03) = 0.45$$

**Example when equal weights are used across assessments**

$$(0.33333 * 0.91) + (0.33333 * 0.65) + (0.33333 * 0.03) = 0.53$$

## Annex 1: Mapping of Security Frameworks and Guidance to Categories

ONSAT’s security categories are used primarily as a common interface to the critical controls and guidance derived from the individual security frameworks. The NIST Cybersecurity Framework (CSF) serves as the umbrella guidance document aligned to ONSAT. A complete mapping of security categories and frameworks is included in the *Security Frameworks Mapping* Tab in the tool. Below is an example of the individual security frameworks mapped to ONSAT’s Security Category 2, System Performance, Resiliency, and Security Architecture and Design Practices.



**Mapping of security frameworks and standards to ONSAT Security Category 2:**

<b>Broad Purpose</b>	Mission Oriented Design of System
<b>Security Category # and Title</b>	Security Category 2: System Performance, Resiliency, and Security Architecture and Design Practices
<b>Functional Description</b>	Build Performance, Resiliency, and Security into the Design of the System

Framework Short Title	Framework Control ID	Framework Control Description / Question	Concatenated Label
CSA	RS-01.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event and properly communicated to tenants?	1 CSA RS-01.1
NIST CSF	ID.AM-5	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	1 NIST CSF ID.AM-5
NIST CSF	ID.BE-1	ID.BE-1: The organization's role in the supply chain is identified and communicated	1 NIST CSF ID.BE-1
NIST CSF	ID.BE-2	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	1 NIST CSF ID.BE-2
NIST CSF	ID.BE-3	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	1 NIST CSF ID.BE-3
NIST CSF	ID.BE-4	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	1 NIST CSF ID.BE-4
NIST CSF	ID.AM-6	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	1 NIST CSF ID.AM-6
NIST CSF	ID.GV-2	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	1 NIST CSF ID.GV-2
NIST CSF	DE.DP-1	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	1 NIST CSF DE.DP-1
NIST CSF	RS.CO-1	RS.CO-1: Personnel know their roles and order of operations when a response is needed	1 NIST CSF RS.CO-1
SEI Illicit Insider	2.2	2.2 Consider all employees, regardless of their technical expertise, when defining security practices and controls.	1 SEI Illicit Insider 2.2
SEI Illicit Insider	3.2	3.2 Consider the enforceability of organizational policies; clearly communicate policies to all employees.	1 SEI Illicit Insider 3.2
Baldrige CS	6.2.4	(4) How do you ensure that your CYBERSECURITY operations consider and align with your organization's overall operations?	1 Baldrige CS 6.2.4
Baldrige CS	6.2.5	(5) How do you ensure that your CYBERSECURITY operations consider and align with your organization's overall operational safety system?	1 Baldrige CS 6.2.5
Baldrige CS	5.1.3	(3) How do you organize and manage your CYBERSECURITY WORKFORCE to establish roles and responsibilities?	1 Baldrige CS 5.1.3
SEI Insider Common Sense	L.4	Implement a clear separation of duties between regular administrators and those responsible for backup and restoration.	1 SEI Insider Common Sense L.4
SEI Insider Common Sense	G.8	8 Enforce separation of duties and least privilege.	1 SEI Insider Common Sense G.8

Framework Short Title	Framework Control ID	Framework Control Description / Question	Concatenated Label
MITRE Cyber Resiliency	RO.1.2	Understand mission or business function dependencies on cyber resources and	1 MITRE Cyber Resiliency RO.1.2
MITRE Cyber Resiliency	RO.7.2	Adapt systems and mission / business processes to mitigate risks	1 MITRE Cyber Resiliency RO.7.2
NIST 800-53-R4	AC-22	Publicly Accessible Content	1 NIST 800-53-R4 AC-22
NIST 800-53-R4	AC-5	Separation of Duties	1 NIST 800-53-R4 AC-5
NIST 800-53-R4	AT-3	Role-Based Security Training	1 NIST 800-53-R4 AT-3
NIST 161	AC-22	Publicly Accessible Content	1 NIST 161 AC-22
NIST 161	AC-5	Separation of Duties	1 NIST 161 AC-5
NIST 161	AT-3	Role-Based Security Training	1 NIST 161 AT-3
ISO 27000	A.6.1.5	Information security in project management	1 ISO 27000 A.6.1.5
ISO 27000	A.14.2.3	Technical review of applications after operating platform changes	1 ISO 27000 A.14.2.3
ISO 27000	A.5.1.1	Policies for information security	1 ISO 27000 A.5.1.1
ISO 27000	A.5.1.2	Review of the policies for information security	1 ISO 27000 A.5.1.2
ISO 27000	A.6.1.1	Information security roles and responsibilities	1 ISO 27000 A.6.1.1
ISO 27000	A.6.1.2	Segregation of duties	1 ISO 27000 A.6.1.2
ISO 27000	A.12.1.1	Documented operating procedures	1 ISO 27000 A.12.1.1

*This is Blank Space*

*This is Blank Space*

## Annex 2: Business Assessment

Verification OR Assessment	Category AND Question	Description of Category and Question/Topic Details
	<b>A</b>	<b>SERVICE PROVIDER IDENTIFICATION</b>
V	1	Company/Business name
V	2	Company Primary Service Provider Location
V	3	Company Primary Service Provider Business Contact
V	4	Company Primary Service Provider Security Contact
V	5	Company Headquarters
V	6	Company Regional Locations Associated with this Service
V	7	Company Major Production Sites Associated with this Service
V	8	Company /Business /Primary Service Provider Notes
	<b>B</b>	<b>BUSINESS OWNER PROFILE</b>
V	9	Publicly or privately held company
V	10	If public, what is the name of the Exchange
V	11	If public, what is the trading symbol
V	12	Type of legal entity and state(s) / nations(s) of incorporation / place of legal organization
V	13	Place of Incorporation / Legal Organization
V	14	Date of Company Inception / Incorporation
V	15	Name of the holding or parent company(s); include ultimate holding or parent company regardless of levels in between your company and parent company
V	16	Name and relationship with subsidiary and owned businesses
V	17	Alternative Doing Business As (DBA) Names
V	18	List the names of the company's executive leadership:
V	19	Identification of Non-U.S. Executives, and Board of Directors with Decision Making Authority Associated with this Service.
V	20	Net Worth of Company
V	21	Volume and Value of Business Per Year
	<b>C</b>	<b>SERVICE PROVIDER PROFILE</b>
V	22	Name and description of services and products to be provided
V	23	Service and Product delivery model
V	24	Providers Participating in Producing / Providing Products / Services
V	25	Primary Location of Production /Provision of Products / Services
V	26	Backup Locations of Production / Provision of Products / Services
V	27	Primary Providers Participating in Providing Data Processing, Storage, and Transmittal Services (Including Internet Service Providers [ISP])
V	28	Primary Locations of Provision of Data Processing, Storage, and Transmittal Services
V	29	Backup Locations of Provision of Data Processing, Storage, and Transmittal Services
V	30	Other Significant Providers, Sites, and Locations Involved in Production / Provision of Products / Services.
	<b>D</b>	<b>MAJOR CHARACTERISTICS OF SERVICE(S) TO BE PROVIDED</b>
A	31	Assessment of Experience in Providing Network Services to Be Considered in this Assessment
A	32	Assessment of Ability to Provide Support to Protect Major Business Functions Affected if Service is Not Provided as Specified
A	33	Assessment of Ability to Protect Identified Sensitive Data Associated with this Service
A	34	Assessment of Ability to Satisfy and Evidence of Compliance with Major Legal Requirements / Issues / Exposure Associated with this Service
A	35	Assessment of Ability to Implement Defined Service Provision
	<b>E</b>	<b>MAJOR SPECIFIC REQUIREMENTS OF SERVICES TO BE PROVIDED</b>
A	36	Assessment of Ability to Satisfy Major Service Level Agreement Performance Specification / Requirements
A	37	Assessment of Ability to Satisfy Major Technical Implementation Specifications / Requirements
A	38	Assessment of Ability to Satisfy Major Interface Implementation Specifications / Requirements
A	39	Assessment of Ability to Satisfy Major Data Access and Privilege Specifications / Requirements
A	40	Assessment of Ability to Satisfy Major Data Confidentiality / Privacy Specifications / Requirements

Verification OR Assessment	Category AND Question	Description of Category and Question/Topic Details
A	41	Assessment of Ability to Satisfy Major Data Integrity Specifications / Requirements
A	42	Assessment of Ability to Satisfy Major Data Availability Specifications / Requirements
A	43	Assessment of Ability to Satisfy Major System / Network Access Specifications / Requirements
A	44	Assessment of Ability to Satisfy Major System / Network Integrity Specifications / Requirements
A	45	Assessment of Ability to Satisfy Major System / Network Availability Specifications / Requirements
A	46	Assessment of Ability to Satisfy Major Physical Access and Privilege Specifications / Requirements
A	47	Assessment of Ability to Satisfy Major Physical Security Specifications / Requirements
A	48	Assessment of Ability to Satisfy Major Personnel Access and Privilege Specifications / Requirements
A	49	Assessment of Ability to Satisfy Major Personnel Security Specifications / Requirements
A	50	Assessment of Ability to Satisfy Major Supply Chain Security and Delivery Specifications / Requirements
A	51	Assessment of Ability to Satisfy Major Subcontractor Provider Specification / Requirements
	<b>F</b>	<b>NON-U.S. INVOLVEMENT AND CONTROL ASSOCIATED WITH SERVICES PROVIDED</b>
A	52	Assessment of Ability to Adhere to and Evidence of Compliance with Restrictions on Non-U.S. Involvement and Control in Provision of Services
A	53	Assessment of Ability to Adhere to and Evidence of Compliance with Special Security Arrangements / Agreements / Separation of Business and Data Activity Accommodations to Satisfy Non-U.S. Involvement and Control Restrictions
A	54	Assessment of Ability to Adhere to and Evidence of Compliance with Reporting and Review Requirements When There Are Changes to the Service Providers, Delivery Model, Contracts, or Special Security Accommodations to Assure Continued Compliance.
A	55	Assessment of Impact on Trust Basis of Non-U.S. Primary Providers Providing the Services and Products
A	56	Assessment of Impact on Trust Basis of Non-U.S. Primary Provider Personnel Providing the Services and Products
A	57	Assessment of Impact on Trust Basis of Non-U.S. Sub-Contractors Providing the Services and Products
A	58	Assessment of Impact on Trust Basis of Non-U.S. Sub-Contractor Personnel Providing the Services and Products
A	59	Assessment of Impact on Trust Basis of Other Non-U.S. Parties Providing the Services and Products
A	60	Assessment of Impact on Trust Basis of Other Non-U.S. Personnel Providing the Services and Products
A	61	Identification and Assessment of Non-U.S. Parties Providing Associated Data Processing, Storage, and Transmittal Services
A	62	Identification and Assessment of Non-U.S. Personnel Providing Associated Data Processing, Storage, and Transmittal Services
	<b>G</b>	<b>BUSINESS RELATIONSHIPS, RELEVANT CLAIMS, JUDGEMENTS, AND REPORTABLE CYBERSECURITY INCIDENTS</b>
A	63	Assessment of business relationships, contracts, or grants with the U.S. Government
A	64	Assessment of business relationships, contracts, or grants with Non-U.S. Governments
A	65	Assessment of business relationships, contracts, or grants with Special Interest Organizations and Individuals
A	66	Assessment of Significant current or past legal claims or judgements that can affect the provision of these services
A	67	Assessment of Significant current or past cybersecurity incidents that can affect the provision of these services
	<b>H</b>	<b>GENERAL REPUTATION AND HISTORICAL TRUST RELATIONSHIP</b>
A	68	Assessment of General Historical Trust Reputation
A	69	Assessment of Direct Historical Trust Relationships
A	70	1) Assessment, Name and Contact Information for service and product references
A	71	2) Assessment, Name and Contact Information for service and product references
A	72	3) Assessment, Name and Contact Information for service and product references
A	73	4) Assessment, Name and Contact Information for service and product references
A	74	5) Assessment, Name and Contact Information for service and product references
A	75	6) Assessment, Name and Contact Information for service and product references



## Annex 3: Security Assessment

Category / Question ID	ONSAT Ref ID	Category / Questions
<b>1</b>	<b>RRR</b>	<b>1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]</b>
1	RRR - 1.1	1) Are Critical Mission/Business Functions Defined and Documented and are Security Requirements and Business Practices Derived and Documented from those Functions?
2	RRR - 1.2	2) Are System Security, Personnel Security, Physical Security and Supply Chain Security Roles and Responsibilities Defined, Documented, Assigned, and Implemented?
3	RRR - 1.3	3) Are documented Security Requirements for Data Confidentiality, Integrity, and Availability, System Integrity and Availability, and Personnel/Process Integrity and Availability, incorporated in both System Design and Business Practices?
4	RRR - 1.4	4) Does corporate management maintain oversight to ensure Mission/Business security requirements are in place as well as authorizing their implementation as well as holding responsible entities accountable?
5	RRR - 1.5	5) Are Mission/Business security requirements incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>2</b>	<b>SDI</b>	<b>2) System Performance, Resiliency, and Security Architecture and Design Practices [System Design]</b>
1	SDI - 2.1	1) Are system and process performance, resiliency and security requirements derived and documented from Critical Mission/Business Functions and effectively incorporated into system designs and management practices?
2	SDI - 2.2	2) Are functions for monitoring, reporting, and responding to anomalous performance, resiliency, and security behavior implemented in system design and procedures to allow for timely response?
3	SDI - 2.3	3) Are functions for monitoring, reporting, and responding to anomalous performance, resiliency, and security behaviors tested and exercised prior to implementation and periodically during operations?
4	SDI - 2.4	4) Are performance, resiliency, and security actively monitored, measured, reported and effectively corrected to assure decision makers that these critical functions a meeting organizational goals and contractual responsibilities?
5	SDI - 2.5	5) Are System Performance, Resiliency, and Security Architecture and Design Practices incorporated into and enforced through service level agreements, contracts, policies, and regulatory practices?
<b>3</b>	<b>DFG</b>	<b>3) Communication Path, Data Flow, and Data Governance Policies and Practices [Data Governance]</b>
1	DFG - 3.1	1) Are Mission/Business critical communication path, data flows, and data governance policies and practices documented and maintained current?
2	DFG - 3.2	2) Are Mission/Business critical communication path, data flows, and data governance policies and practices incorporated into the operations and handling of Mission/Business critical information?
3	DFG - 3.3	3) Is Mission/Business critical information labeled, tagged, and securely associated with appropriate metadata to allow for and promote effective enforcement of Data Governance Policies and Practices
4	DFG - 3.4	4) Are Data Governance incidents and violations actively monitored, reported, and effectively corrected?
5	DFG - 3.5	5) Are Communication Path, Data Flow, and Data Governance Policies and Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?

<b>4</b>	<b>AIA</b>	<b>4) Asset Inventory and Audit Management Practices [Asset and Audit]</b>
1	AIA - 4.1	1) Are Mission/Business Critical operational assets inventoried and periodically audited to assure their initial and continued pedigree, accountability and integrity?
2	AIA - 4.2	2) Are Mission/Business Critical backup, reserve, and replacement assets inventoried, and periodically audited to assure their initial and continued pedigree, accountability and integrity?
3	AIA - 4.3	3) Are Asset Inventory and Audit data protected from loss, corruption, or manipulation, and are asset inventory and audit data available for use and incorporated into defining the integrity of the Mission/Business critical functions and processes?
4	AIA - 4.4	4) Are Asset Inventory and Audit data reviewed and assessed to support an effective known configuration of the system and processes and effective and timely corrective actions?
5	AIA - 4.5	5) Are Asset Inventory and Audit Management Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>5</b>	<b>AAC</b>	<b>5) Authentication and Access Control Practices [Info. Sys.Security]</b>
1	AAC - 5.1	1) Are identities of authorized individuals documented and vetted, and are credentials validated to support effective physical and electronic access and privilege management to Mission/Business critical information, services, and assets?
2	AAC - 5.2	2) Are credentials protected from loss, misuse, and manipulation?
3	AAC - 5.3	3) Are the processes for assessing and allowing access and privilege based on credentials documented, incorporated, and trained? Do these processes assure that only authorized individuals and entities have access and privilege to Mission/Business Critical Information, Services, and Assets?
4	AAC - 5.4	4) Are Access and Privilege incidents and violations actively monitored, reported, and effectively corrected?
5	AAC - 5.5	5) Are Authentication and Access Control Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>6</b>	<b>NSP</b>	<b>6) Network Segmentation Practices [Info. Sys.Security]</b>
1	NSP - 6.1	1) Are Mission/Business Critical Networks logically, physically, or cryptographically separated to support only authorized access to specific classes of information, functions, or services? (Test vs. Operational Separation; Information Class Separation; Function or Service Separation)
2	NSP - 6.2	2) Are Authentication and Access Control Processes Defined, Documented, Incorporated and Implemented? Do Authentication and Access Control support Network Segmentation?
3	NSP - 6.3	3) Are your network interfaces Defined, Controlled and Protected from unauthorized access?
4	NSP - 6.4	4) Are Network Separation incidents and violations actively monitored, reported, and effectively corrected?
5	NSP - 6.5	5) Are Network Segmentation Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>7</b>	<b>CIA</b>	<b>7) Data Confidentiality, Integrity and Availability Protection Practices [Info. Sys.Security]</b>
1	CIA - 7.1	1) Are Cybersecurity Practices Defined, Documented, Incorporated and Implemented to protect the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets?
2	CIA - 7.2	2) Are Mission/Business Critical Information, Functions, Services, and Assets Identified and Documented to support effective positive and negative access control through Data Confidentiality, Integrity, and Availability Protection Practices?
3	CIA - 7.3	3) Are Cryptographic and Key Management Processes managed and assessed to support effective positive and negative access control through Data Confidentiality, Integrity, and Availability Protection Practices?

4	CIA - 7.4	4) Are Data Confidentiality, Integrity, and Availability Protection incidents and violations actively monitored, reported, and effectively corrected?
5	CIA - 7.5	5) Are Data Confidentiality, Integrity, and Availability Protection Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>8</b>	<b>VRM</b>	<b>8) Vulnerability and Resilience Management Practices [Info. Sys.Security]</b>
1	VRM - 8.1	1) Are Vulnerability and Resilience Management Practices defined, documented, incorporated, and implemented to prevent and detect exploitation, modification, or denial and preservation of Mission/Business Critical Information, Functions, Services, and Assets through routine and crisis operations?
2	VRM - 8.2	2) Are vulnerability scans conducted and update patches and corrections documented and implemented to prevent and reduce opportunities for vulnerability exploitations that lead to the loss of Confidentiality, Integrity, or Availability of Mission/Business Critical Information, Functions, Services, and Assets through routine and crisis operations?
3	VRM - 8.3	3) Are backup, recovery, and continuity of operations (COOP) practices defined, documented, and incorporated into the system design and operating procedures to support timely continuity of availability of Mission/Business critical Information, Functions, Services, and Assets through routine and crisis operations?
4	VRM - 8.4	4) Are Vulnerability and Resilience Management incidents and violations actively monitored, reported, and effectively corrected?
5	VRM - 8.5	5) Are Vulnerability and Resilience Management Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>9</b>	<b>CMP</b>	<b>9) Configuration Management Practices [Info. Sys.Security]</b>
1	CMP - 9.1	1) Are Configuration Management Practices defined, documented, incorporated, and implemented to prevent the introduction (accidental or intentional) of vulnerabilities that can lead to the failure or exploitation of Mission/Business Critical Functions, Services, and Assets?
2	CMP - 9.2	2) Are current system and process configurations documented and updated, and changes evaluated, approved, coordinated and implemented to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
3	CMP - 9.3	3) Is the integrity and effectiveness of replacement parts and design changes reviewed and tested prior to implementation to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
4	CMP - 9.4	4) Are Configuration Management incidents and violations actively monitored, reported, and effectively corrected?
5	CMP - 9.5	5) Are Configuration Management Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
<b>10</b>	<b>SMR</b>	<b>10) System Maintenance and Repairs Practices [Info. Sys.Security]</b>
1	SMR - 10.1	1) Are System Maintenance and Repair Practices defined, documented, incorporated, and implemented to prevent the introduction (accidental or intentional) of vulnerabilities that can lead to the failure or exploitation and to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
2	SMR - 10.2	2) Are System Maintenance and Repair personnel identified and vetted, and are repair procedures and implementations documented, reviewed, inspected, and tested to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
3	SMR - 10.3	3) Are the integrity and effectiveness of repair parts and design changes reviewed, tested and evaluated prior to implementation to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
4	SMR - 10.4	4) Are System Maintenance and Repair Practice incidents and violations actively monitored, reported, and effectively corrected?
5	SMR - 10.5	5) Are System Maintenance and Repair Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?



11	IDR	11) Incident Detection and Response [Info. Sys. Security]
1	IDR - 11.1	1) Are Incident Detection and Response Practices defined, documented, incorporated, and implemented to prevent the introduction (accidental or intentional) of vulnerabilities that can lead to the failure or exploitation and to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
2	IDR - 11.2	2) Are Incident Detection and Response practices coordinated and are personnel trained, and procedures exercised to assure timely and effective incident response to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
3	IDR - 11.3	3) Are after action assessments conducted, documented, and improvements leveraged to improve the processes, procedures, documentation, training, and implementation of Incident Detection and Response Practices to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
4	IDR - 11.4	4) Are potentially harmful incidents detected, actively monitored, reported and mitigated to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
5	IDR - 11.5	5) Are Incident Detection and Response Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
12	CIR	12) Consequence / Impact Recovery Policies and Practices [Info. Sys. Security]
1	CIR - 12.1	1) Are Consequence / Impact Recovery Practices defined, documented, incorporated, and implemented to minimize the damage associated with failures, accidents, natural disasters, and intentional attacks and to restore operational capability and integrity of Mission/Business Critical Information, Functions, Services, and Assets?
2	CIR - 12.2	2) Are the direct technical and procedural effects of failures, accidents, natural disasters, and intentional attacks documented and mapped to their broader operational effects on the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets and ultimately to Mission/Business operations?
3	CIR - 12.3	3) Are Mission/Business Continuity of Operations plans and policies documented and incorporated, personnel trained, procedures exercised, and backup, recovery, and reconstitution assets invested in, protected, and tested to assure the continued integrity and operational availability of Mission/Business Critical Information, Functions, Services, and Assets?
4	CIR - 12.4	4) Are Consequence / Impact Recovery Policy and Practice incidents and violations actively monitored, reported, and effectively corrected?
5	CIR - 12.5	5) Are Consequence / Impact Recovery Policy and Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
13	PFS	13) Physical / Facilities Security Policies and Practices [Physical Security]
1	PFS - 13.1	1) Are physical/facilities security policies and practices defined, documented, and incorporated into the processes, procedures, documentation, training, and implementation of Physical / Facilities Security Policy and Practices to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
2	PFS - 13.2	2) Are Physical / Facilities Security Policies and Practices implemented and coordinated with Information Security and Personnel Security practices to provide an effective and coordinated ability to preserve the Confidentiality, Integrity, and Availability of Mission/Critical Information, Functions, Services, and Assets?
3	PFS - 13.3	3) Are Physical / Facilities Security Policies and Practices assessed and are personnel trained, and procedures exercised to assure timely, effective, and coordinated incident response to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
4	PFS - 13.4	4) Are Physical / Facilities Security Policy and Practice incidents and violations actively monitored, reported, and effectively corrected?
5	PFS - 13.5	5) Are Physical / Facilities Security Policy and Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?



14	PSP	14) Personnel Security Policies, Awareness, and Training [Personnel Security]
1	PSP - 14.1	1) Are Personnel Security Policies and Practices defined, documented and incorporated into the processes, procedures, documentation, training, and implementation of Personnel Security Policy and Practices to ensure that only vetted and authorized personnel with requisite knowledge and skills have access to Mission Critical/Business Critical information, functions, services, and Assets? And to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
2	PSP - 14.2	2) Are Personnel Security Policies and Practices coordinated with Information Security and Physical Security practices to provide an effective and coordinated ability to preserve the Confidentiality, Integrity, and Availability of Mission/Critical Information, Functions, Services, and Assets?
3	PSP - 14.3	3) Are Personnel Security Policies and Practices assessed, personnel trained, and procedures exercised to assure the identity and trustworthiness of employees, contractors, maintenance and service personnel, and visitors with physical or logical access to Mission/Business Critical Information, Functions, Services, and Assets?
4	PSP - 14.4	4) Are Personnel Security Policy and Practice incidents and violations actively monitored, reported, and effectively corrected?
5	PSP - 14.5	5) Are Personnel Security Policy and Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
15	PMP	15) Performance Management Practices [System Governance]
1	PMP - 15.1	1) Are Performance, Confidentiality, Integrity, and Availability practices documented and implemented in a balanced manner to meet Security and Business Critical operations and contractual obligations through routine and crisis situations?
2	PMP - 15.2	2) Are Mission/Business Critical operations and associated performance levels defined and incorporated into the corporate management practices to preserve the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets?
3	PMP - 15.3	3) Are Mission/Business Critical operations and associated performance levels trained and exercised by all personnel to preserve the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets?
4	PMP - 15.4	4) Are System Performance, Information Confidentiality, Information Integrity, and Information Availability measured to assure decision makers that these critical functions a meeting organizational goals and contractual responsibilities?
5	PMP - 15.5	5) Are Performance Management Practices (System Governance) incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
16	GRC	16) Governance, Risk, and Compliance (GRC) Management Practices [System Governance]
1	GRC - 16.1	1) Are Governance, Risk, and Compliance (GRC) Management Practices defined, documented and incorporated into the corporate management practices to preserve the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets?
2	GRC - 16.2	2) Are Governance, Risk, and Compliance (GRC) Management Practices implemented, coordinated, trained, and corporately managed to meet Mission/Business Critical operations and obligations through routine and crisis situations?
3	GRC - 16.3	3) Are Governance, Risk, and Compliance (GRC) policies, requirements, and obligations and their implementation effectively incorporated into the decision-making culture and management practices throughout the organization?
4	GRC - 16.4	4) Are Governance, Risk, and Compliance (GRC) Practices measured to assure decision makers that these critical functions are meeting organizational goals, contractual responsibilities, and legal and regulatory requirements?
5	GRC - 16.5	5) Are Governance, Risk, and Compliance (GRC) Management Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?

17	AIP	17) Asset HW/SW Integrity Protection Practices [Supply Chain]
1	AIP - 17.1	1) Are Asset HW/SW Integrity Practices documented and incorporated to prevent the accidental or intentional introduction of vulnerabilities that can lead to the failure or exploitation of Mission/Business Critical Functions, Services, and Assets?
2	AIP - 17.2	2) Are current Asset HW/SW performance and integrity specifications documented and updated, and changes evaluated, approved, and implemented to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
3	AIP - 17.3	3) Are the performance and integrity characteristics of Asset HW/SW assessed and tested prior to implementation to preserve the integrity of Mission/Business Critical Information, Functions, Services, and Assets?
4	AIP - 17.4	4) Are Asset HW/SW incidents and violations actively monitored, reported, documented, and effectively corrected?
5	AIP - 17.5	5) Are Asset HW/SW Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?
18	SDV	18) Supplier Documentation and Vetting Policy and Practices [Supply Chain]
1	SDV - 18.1	1) Are Supplier Documentation and Vetting Policy and Practices implemented and coordinated with Information Security and Physical Security practices to provide an effective and coordinated ability to preserve the Confidentiality, Integrity, and Availability of Mission/Critical Information, Functions, Services, and Assets?
2	SDV - 18.2	2) Are Supplier Documentation and Vetting Policy and Practices documented, personnel trained, and procedures exercised to assure the integrity of products and services provided by this Supplier to preserve the Confidentiality, Integrity, and Availability of Mission/Critical Information, Functions, Services, and Assets?
3	SDV - 18.3	3) Are Supplier Documentation and Vetting Practices incorporated into processes, procedures, documentation, training, and implementation of Supplier Documentation and Vetting Practices to preserve the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets?
4	SDV - 18.4	4) Are Supplier Documentation and Vetting Policy and Practice incidents and violations actively monitored, reported, and effectively corrected?
5	SDV - 18.5	5) Are Supplier Documentation and Vetting Policy and Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?

## Annex 4: Tool Settings Adjustment

The “Tool Adjustment Settings” section of the tool contains 10 individual tabs that can be used to modify the content and/or weight of the questions and categories, the weight of the overall assessments, and/or the scale values and format. To change a default value, open up the individual tab that applies e.g. Business Category Weights and enter a value in the User Defined Value field. Once saved in the individual tab, the change is reflected in the *User Defined What If Values* Tab. In this manner, the *User Defined What If Values* Tab acts as a Default Settings Tab for User Defined Values.

User Defined "What If" Values		
Decision Criteria and Scale	Business	Security
<ul style="list-style-type: none"> <li>• Decision Criteria-Weight Definition</li> <li>• Scale Format Definition</li> </ul>	<ul style="list-style-type: none"> <li>• Business Category Definition</li> <li>• Business Questions Definition</li> <li>• Business Category Weights</li> <li>• Business Question Weight</li> </ul>	<ul style="list-style-type: none"> <li>• Security Category Definition</li> <li>• Security Questions Definition</li> <li>• Security Category Weights</li> <li>• Security Question Weights</li> </ul>

Uses of weights are as diverse as the scenarios being assessed.

- Example 1: As an outsourcing company, your business practices are at a Level 5 Very High Trust Basis but the maturity of your implemented security practices is a Level 2 Limited, and Undefined. Weighting the Security Maturity Assessment higher than the Business Trust Assessment, will aid in identifying a service provider strong in security practices to complement your company.
- Example 2: Your company is reviewing its internal supply chain processes. Within the security maturity assessment, you weight categories 17 - Asset HW/SW Integrity Protection Practices [Supply Chain] and 18 - Supplier Documentation and Vetting Policy and Practices [Supply Chain] higher than the other categories to expose gaps in your supply chain practices.
- Example 3: Your company's executive team have asked for a larger score span for the business trust assessment. One way to do this is to change the scale level values to increase the numerical distance between the levels:
  - Change Level 1 from 0.20 to 0.15
  - Change Level 2 from 0.50 to 0.35
  - Change Level 3 from 0.75 to 0.70
  - Leave Level 4 at 0.85
  - Change Level 5 from 0.95 to 1.0

*This is Blank Space*

**End of Document**