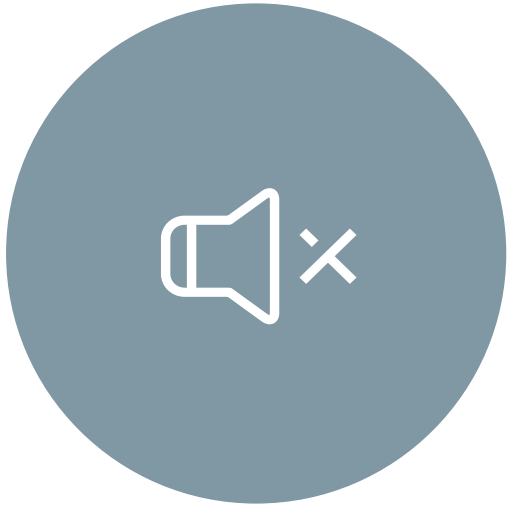
Thank you for joining:

Maximizing Value Through Establishing Great IIS Contract Agreements

If you experience any technical issues during the meeting, please contact Jo Turcotte via direct message in the Chat.

Logistics

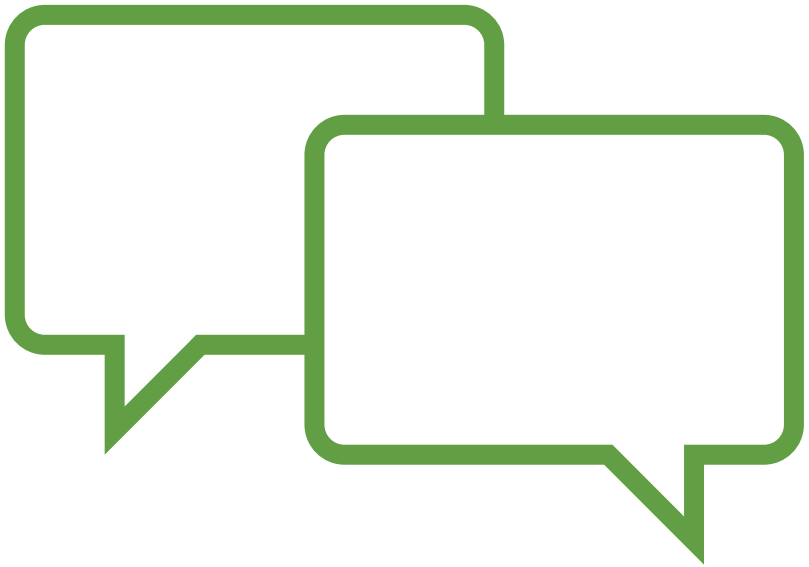
This meeting is being recorded and will be posted in the AIRA repository



All phone lines are muted

Technical Support

If you experience any technical issues during the meeting, please contact **Jo Turcotte** via direct message in the Chat.



ENVISION TECHNOLOGY PARTNERS

Maximizing Value Through Establishing Great IIS Contract Agreements

Gary Wheeler, Executive Vice President and General Manager

September 27, 2023

What makes a great contract?

- Clarity
- Mutually beneficial

Goal Today

Take a high-level, non-legal, vendor-agnostic look at contracts (beyond products and services) sharing potential risks and barriers that could result in increased prices, inability to execute a contract renewal, or limited competition.

ENVISION TECHNOLOGY PARTNERS

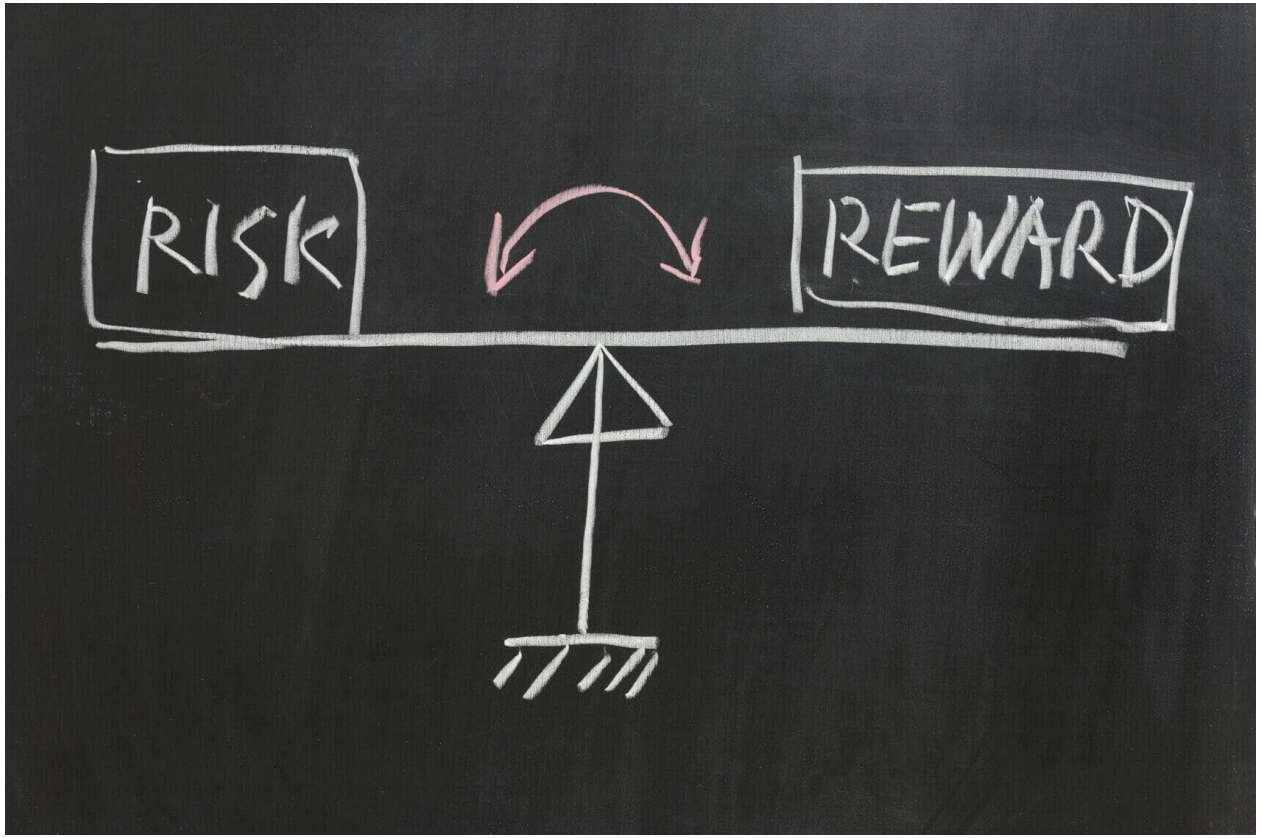
Areas of Focus

- ❑ Contract Terms and Conditions
- ❑ Service Level Agreements
- ❑ Security Audit Requirements
- ❑ IIS Product and Delivery Requirements
- ❑ Strategies
- ❑ Resources

ENVISION TECHNOLOGY PARTNERS

A couple fundamentals…

- **All aspects** of a contract have potential impact on price and ability to participate
- When contract issues arise, **IIS programs may not be in control**



Potential Showstoppers

Liability

- Unlimited liability risks
- Specific clause example:

> *"The Supplier shall cooperate with any litigation and investigation to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll-free telephone call center services."*

Credit Monitoring is ~$100/year/person; $300 total/person

$300/person * 4M (population) = **$1.2B obligation** for breach credit monitoring

Potential Showstoppers

Insurance

- As policy limits increase, costs increase affecting price
- Unattainable limits for cyber liability insurance

Tiered Coverage Schedule

Level	Number of PII records	Level of cyber liability insurance required (occurrence = data breach)
1	1-10,000	$2,000,000 per occurrence
2	10,001 – 50,000	$3,000,000 per occurrence
3	50,001 – 100,000	$4,000,000 per occurrence
4	100,001 – 500,000	$15,000,000 per occurrence
5	500,001 – 1,000,000	$30,000,000 per occurrence
6	1,000,001 – 10,000,000	$100,000,000 per occurrence

Notes:

Most insurers only insure a maximum policy of $5m and companies typically reach higher limits through retaining multiple policies and may not be attainable at a population level.

Potential Showstoppers

Other Areas (typically aligned to custom development)

- ❑ Intellectual Property (IP)/Ownership Rights, COTS Product Considerations
- ❑ Warranties
- ❑ State-specific IT Terms and Conditions - (specifically change management)

Language Barriers

- Some language areas that might need working through are:
  - ‘Including but not limited to’
  - ‘Sole discretion of client’
  - ‘Industry Best Practices’
  - ‘Indemnification’

Service Level Agreements (SLAs)

- ❑ Value of SLAs
  - ✓ Protects both parties
  - ✓ Establishes standards and expectations
  - ✓ May define consequences for unmet obligations

- ❑ Typical IIS SLA Categories
  - ✓ IIS Availability
  - ✓ IIS Response Time
  - ✓ Vendor Response Time
  - ✓ Vendor Resolution Time (difficult)

SLA Considerations

- ❑ Keep SLAs **Measurable**
- ❑ Keep **SLAs Focused** - every SLA you have needs to be monitored and reported adding administrative costs
- ❑ Vendor **Relationship Impacts** - consider writing SLAs that work up to a financial penalty and equally weighs impacts
- ❑ Product purchases, many have **Standard COTS SLAs** - see if those meet needs as modifications to client-specific SLAs may have cost implications
- ❑ **24x7 Support?** - consider what is required outside standard business day for response time and responses (e.g., costly for eyes on glass, US-based resources)
- ❑ **Direct Cost Correlation** - as service level expectations increase, so does cost

Security Audits and Reporting

Key areas to understand include:

- What type of ongoing security audit, if any, is required?
  - Is a vendor self-assessment sufficient?
  - Are there client-specific forms vendor needs to complete?
  - Is there a client security review board that needs to approve implementation?
  - Is an independent third-party audit (such as penetration testing or SOC2) required?

Security Audits and Reporting – SOC2 Type II

- Systems and Organization Controls (SOC)2 – Comprehensive report framework from AICPA in which third-party auditors assess and test criteria for Security, Availability, Processing Integrity, Confidentiality, and/or Privacy
- Considerations
  - Environment vs. Application/Product
  - Duration
  - Cost

Product/Delivery Requirements

- ❑ Value of consistency in IIS functional standards at national level utilizing PHII's Requirement Traceability Matrix Requirements – PHII

Immunization Information System (IIS) Baseline Requirements Traceability Matrix (RTM)

Admin System	Requirements related to the function: Administer System
Manage Orgs	Requirements related to the function: Manage Organizations and Facilities
Manage Users	Requirements related to the function: Manage Users
Interop	Requirements related to the function: Support Interoperability
Data Quality	Requirements related to the function: Ensure Data Quality
Eval Forecast	Requirements related to the function: Evaluate & Forecast
Manage Pt Iz Record	Requirements related to the function: Manage Patient & Immunization Records
Manage Vaccine Inventory	Requirements related to the function: Manage Vaccine Inventory
Data Access	Requirements related to the function: Provide Data Access
Non-functional	Technical requirements across key attributes
Glossary	List of terms used in requirements and their definitions
Crosswalk to FS	Compare the Functional Model to the IIS Functional Standards.

This RTM was developed by the Public Health Informatics Institute, in partnership with AIRA and CDC and with financial support from CDC under Cooperative Agreement number 6- NU38OT000316. Questions, comments and suggestions are welcomed at iis@phii.org.

Public Health Informatics Institute

ENVISION TECHNOLOGY PARTNERS

Strategies

- Education on IIS/Services to IT/Legal/Procurement - where possible developing relationships and highlight impacts of not having an IIS support contract
- Renewals, leverage current T&Cs wherever possible – items may have changed but typically easier starting point
- Information to your vendor as early as possible
- Prepare for redlines and plan for multiple iterations between parties
- Conversations expedite resolution over redlines
- Positive attitude, nothing is impossible

Resources

- ❑ PHII IIS Learning Hub IIS Hub – PHII including IIS Requirements – PHII
- ❑ AIRA Community
- ❑ CDC IIS SME

Question & Answer

How do I ask a question?

Select the unmute icon and ask your question verbally.

Select the chat icon and type your question into the chat box.

Select the reactions icon, select “Raise Hand,” and you will be called on.

Thank you to our presenter, and thanks to all of you for joining us!