NEW YORK STATE OF OPPORTUNITY. | NY GovBuy

co-sponsored by

NEW YORK STATE OF OPPORTUNITY. Office of General Services

Effective Terms and Conditions for the Digital Age

SAMPO NIGP CHAPTER

SUNY

Boards of Cooperative Educational Services BOCES of NEW YORK STATE

May 4 & 5, 2022

Presenters

- Hannah Schmidt
- Jordan Flores

Lesson 1:

Acquire & Review Information

@NYS_OGS @NewYorkStateOGS #2022NYGovBuy

NEW YORK STATE OF OPPORTUNITY. | NY GovBuy

Cloud Types

Let us start by reviewing some examples of cloud products

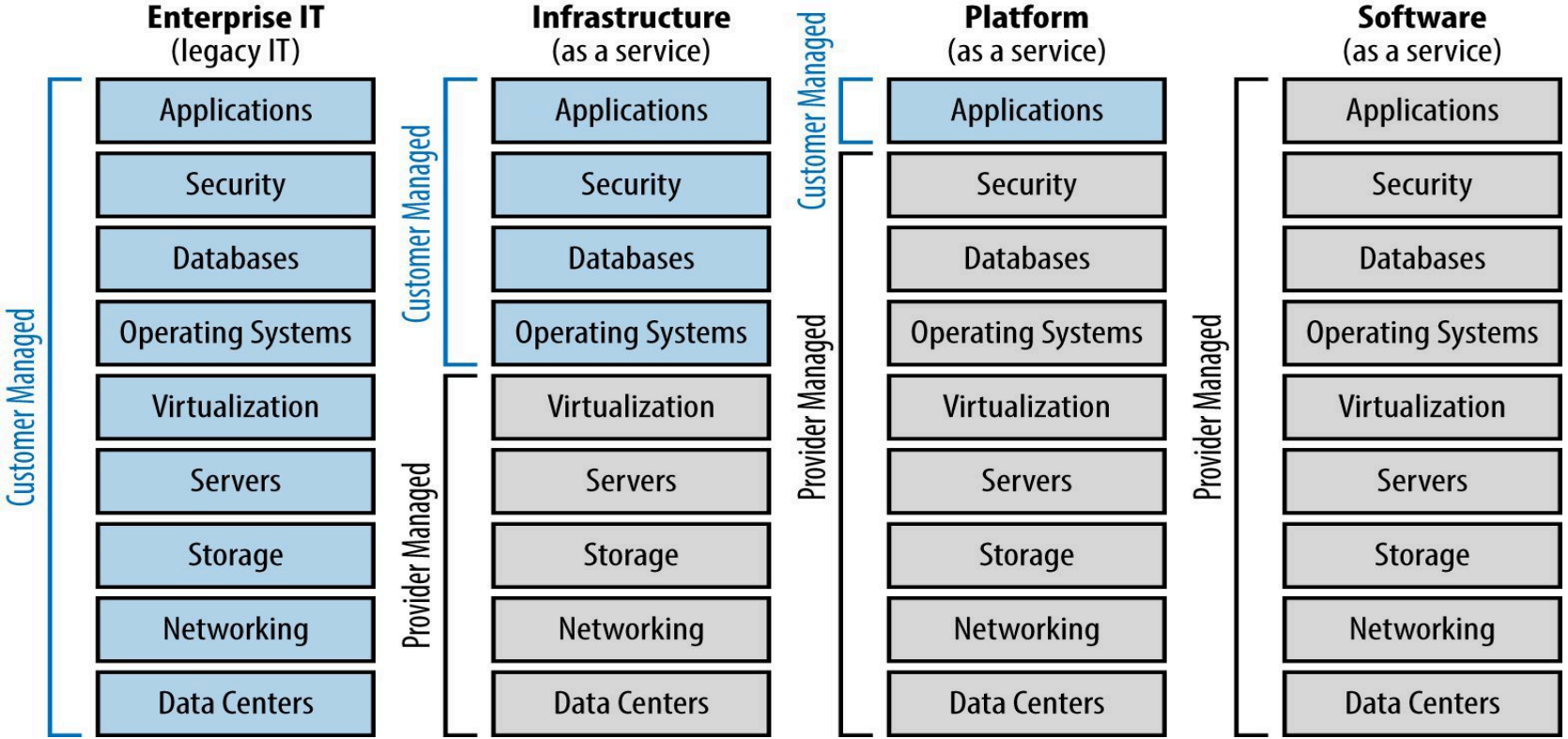
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Anything as a Service (XaaS)

Cloud Types

- SaaS
  - Also known as cloud-based software
  - Software is made available over the internet
  - Completely managed by the vendor
- PaaS
  - The user manages the applications in the service - the rest is managed by the vendor
  - Includes hardware and software tools and resources over the internet

Cloud Types

- IaaS
  - User provides everything from the operating system on up
  - Often used for custom applications
- XaaS
  - General term that refers to the delivery of anything
  - For example, Security as a Service or Healthcare as a Service


Enterprise IT
(legacy IT)
Customer Managed
Applications
Security
Databases
Operating Systems
Virtualization
Servers
Storage
Networking
Data Centers
Infrastructure
(as a service)
Customer Managed
Provider Managed
Applications
Security
Databases
Operating Systems
Virtualization
Servers
Storage
Networking
Data Centers
Platform
(as a service)
Customer Managed
Provider Managed
Applications
Security
Databases
Operating Systems
Virtualization
Servers
Storage
Networking
Data Centers
Software
(as a service)
Provider Managed
Applications
Security
Databases
Operating Systems
Virtualization
Servers
Storage
Networking
Data Centers

Cloud Types

- Single tenant
- Multi-tenant
- Fully hosted
- Hybrid hosted

Cloud Types

- **Single tenant**:
  - When an entity is the only tenant being serviced by a software instance within the cloud
  - This typically results in a higher price

- **Multi-tenant**:
  - Occurs when one instance of the software is serving multi-tenants or entities
  - While this option certainly costs less due to the shared architecture and databases, it is not as secure

Cloud Types

- **Fully hosted:**
  - Requires the supplier to provide the hardware space, software, maintenance, and services
  - May require separate agreements that reference each other
- **Hybrid hosted:**
  - Could result in the vendor providing hardware to the user, or the user may use their own hardware that runs the software and stores data at the user's site
  - Some of the software is hosted in the cloud while some is hosted on-site

Business Drivers

- A business driver is a resource, process or condition that is vital for the continued success and growth of a business

- A company must identify its business drivers and attempt to maximize any that are under their control

  - Needs and costs
  - Infrastructure
  - Access
  - Security
  - Flexibility

Business Drivers – Need and Cost

- **Is there a real need for moving to the cloud?**
  - Is there a solid business driver or is it simply a new and exciting product?

- **Are there real cost savings?**
  - Cost savings should take into consideration possible additional costs such as:
    - Maintaining a failover infrastructure
    - Maintaining a secondary cloud service

Business Drivers – Infrastructure & Access

- **Can the current infrastructure support the cloud?**
  - Is there sufficient processing server power, storage space, bandwidth, network availability, uptime and stability, and security?

- **What is the need for accessibility or availability?**
  - Consider how critical the application is to the business unit.
  - What are the consequences if it is down for five minutes, an hour, a day, a week?

Business Drivers – Security

- **Is the organization able to provide the security requirements needed to facilitate the cloud solution?**
  - Does the cloud solution require special clearances, building modifications, etc.?
  - What does the cloud solution require that the organization does not have or chooses not to provide?

Business Drivers - Flexibility

- **Do we need flexibility?**
  - Flexibility typically comes in two methods:
    - Pay for capability
    - “Ratchet up”
  - Typically, the cloud supplier can spread the cost over many customers, but sometimes you are the “loss leader”

Stakeholders

- Stakeholders are:
  - Those people/departments that will help you research and gather information
  - Those that you will need approvals/buy-in from in order to proceed

- To work effectively, you all must be on the same page

Various Types of Stakeholders

- **Strong technical knowledge**
  - Work with them to get well-considered requirements
- **Political, not technical**
  - The political side is often moved by forces not related to technical needs
  - This may include economic or social considerations
  - Factors such as experience or successful track record do not always enter the discussion
- **Not political, not technical**
  - Typically, the easiest to work with
  - Can take considerable time due to being research intensive

Obtaining Approvals

- **Information security officer (ISO)**
  - Individual responsible for maintaining operational security
  - Ensures the client has done the appropriate homework regarding data and data security
- **Budget officer (BO)**
  - Individual responsible for ensuring the client has the financial means for the purchase
  - Budgeting for cloud products is different than budgeting for other technology products:
    - Configuration errors are easy to make and can lead to additional costs
    - Monitoring is necessary as improper usage can also lead to additional costs

Obtaining Approvals

- **Project manager (PM)**
  - Cloud project management differs from standard software implementation and management. Cloud PMs must:
    - Ensure that failover is held in consideration
    - Remember a cloud provider's business model is to make it hard to for a customer to leave, therefore tools and structures for exits should be built in from day one
    - Understand and retain the cloud life cycle process

Gauging Stakeholders' Understanding

- Cloud types
- Security
- Time frame
- Data location
- Data classification
- Access to data

Gauging Stakeholders' Understanding – Cloud Type

- **What type of cloud is it?**
  - Can they describe the solution fully enough to build requirements?
  - Is it IaaS, PaaS, SaaS, XaaS, single vs. multi-tenant, full vs. hybrid hosted?
- **Private or public cloud?**
  - Private cloud: your data is separated from everyone else's
    - You have a great deal of control over a private cloud
  - Public cloud: your data may be mingled or logically separated

Gauging Stakeholders' Understanding – Security and Timeframe

- **What laws or security provisions apply?**
  - For example, all governmental entities are responsible to meet the National Institute of Standards and Technology (NIST) guidelines
  - Specific types of data have specific rules

- **What is the timeframe?**
  - Cloud can be faster to deploy than software
  - Cloud systems rarely adapt to user's processes
  - Modification of procedures may require a lengthy process

Gauging Stakeholders' Understanding – Data Location

- **Does data have to stay in the continental United States (CONUS)?**
  - Data may need to stay in the CONUS for security reasons
    - However, what security factors are gained by keeping data in the United States?
    - Is CONUS required for legal reasons?
  - Unless CONUS is required by law, you may be significantly overpaying
    - You also may be restricting excellent options from your pool of potential offerors

Gauging Stakeholders' Understanding – Data Classification

- Used to help determine what data you have and what risk that data may pose
- The tool poses a series of questions to determine what risk the release of the data would have
  - Monetary
  - Political
  - Reputational
  - Trust
- The key is the team must know their data and know what laws apply

Gauging Stakeholders' Understanding – Access to Data

- **Who can access the data?**
  - Reach an understanding with your cloud supplier and reseller for who can access the data
  - You must consider how they are background checked, how they are trained, etc.

Research

- Suppliers
- Total cost of ownership
- Risks vs. Rewards

Research - Suppliers

- Verify what suppliers say they can do
  - Dominant suppliers
    - Determine the dominant suppliers in the U.S. and who their customers are
    - Get a feel for where your need fits in the marketplace
  - Other suppliers
    - Determine the advantages of a major supplier versus other suppliers
    - Also determine the trend services are moving towards

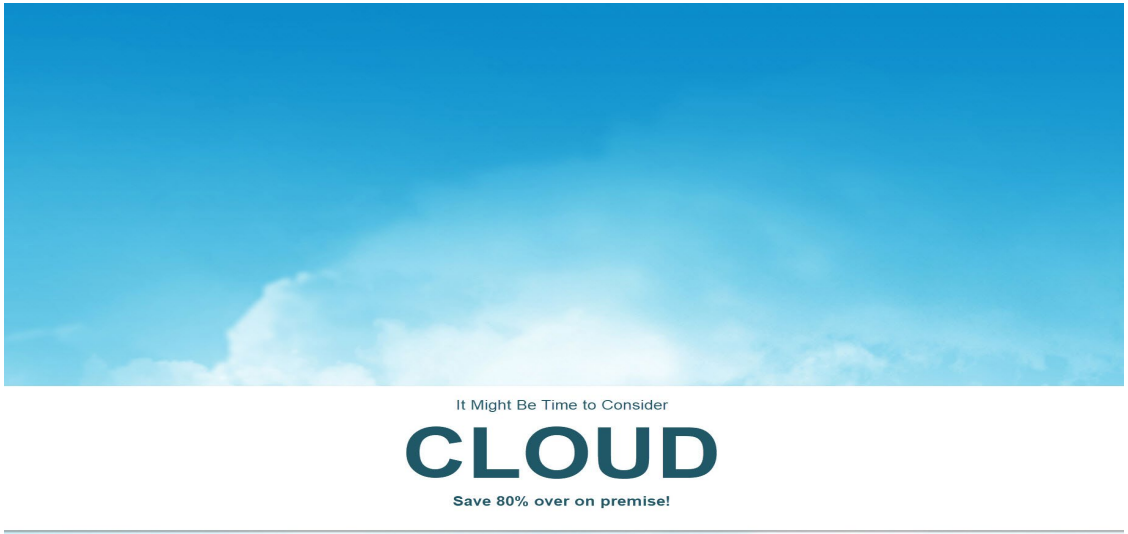
Research - Total Cost of Ownership

- **Hard Costs**
  - Generally, hard costs are costs that are fixed
  - Costs of the product itself - these may be one-time only costs or yearly recurring costs
  - You may need to pay for storage
- **Soft Costs**
  - Soft costs are costs that are variable
  - A cloud system rarely is built for you; you must adapt to fit it
  - There are process reengineering costs, retraining costs, form conversion costs, data conversion costs, and other costs at making your system fit to a new solution

Research - Risks vs. Rewards

- Some rewards for going into cloud include:
  - Cost savings
  - Handing problems over
  - Cloud is new and exciting
- Some risks for going into cloud include:
  - Cloud advertisements
  - Business continuity
  - Cost of going cloud
  - Cloud is confusing
  - Handing over data – privacy and security
  - Potential loss of data
  - High cost to leave

Risk - Cloud Advertisements



NEW YORK STATE OF OPPORTUNITY. | NY GovBuy

Risk - Business Continuity

- The vendor's business continuity/disaster recovery plan may say that they are back up and running in 4 - 6 hours
  - Does not mean your application will be back up in that time frame
  - The time it takes depends on factors such as:
    - Customer size – the # of users
    - Expansiveness of the cloud system
  - During the outage, any data entered may be lost
    - Depending on the terms, the loss of data may not be the responsibility of the cloud supplier

Risk – Cost of Going Cloud

- First look at cost and start with a cost benefit analysis
- In general, cloud does save you money with some precautions:
  - Critical systems should be mirrored by a second supplier or environment
  - A failover infrastructure may need to be maintained
  - Security analysis and periodic review are critical

Risk - Privacy and Security

- Your data is valuable
- The information it contains can be invaluable
  - To mitigate this:
    - Have your security stakeholders involved on day one
    - Have contractual terms and a clear understanding of who is responsible for what at all times
    - Ensure good background check policies are in place
    - Ensure strong encryption is implemented whenever the data is accessed or moved in quantity
    - Get immediate notification upon incident or breach

Risk – Potential Loss of Data

- Suppliers may not be liable for lost data
- Even the most expensive cloud solution in which they mirror the data can still lose data in the transition
- You may still want to keep an infrastructure on hand
  - A rule of thumb is enough to support your 2 - 3 most compute intensive applications running at maximum load simultaneously
- Remember they are sharing their source code with you, so they are taking a risk on you as well

Risk - High Cost to Leave

- Data may belong to a supplier at the end of a service term and customers do not have negotiating power at that point
- This risk can be mitigated with language added to terms and conditions
- Even if you have language to retain ownership, suppliers may have created additional exit services
  - These may include data extraction specialists, data transfer technicians, or even data line fees for removal of data

Risk - Cloud is Confusing

- The cloud is not a clearly defined space
  - Jurisdictions change and rules change constantly.
  - If you give them your data, can you get it back, who will they share it with?
  - What's the total cost of going Cloud?
  - How do I avoid loss of data?
- All these risks can only be controlled in two ways:
  1. Strong contract terms
  2. Good vetting practices

Lesson 2:

Develop the Cloud RFP

@NYS_OGS @NewYorkStateOGS #2022NYGovBuy

NEW YORK STATE OF OPPORTUNITY. | NY GovBuy

Determining Factors

- There are three major determining factors for cloud procurements
  - Laws
    - Where can data go?
    - What level does data have to be stored at?
  - Features & requirements
    - Work with clients to determine the requirements
    - Then determine if it exists
  - Pricing structure
    - To issue a solicitation, you want to be able to do an apples-to-apples comparison when you get offers
    - To do that, you need to understand the pricing, or the structure of pricing

Consider Other Methods

- Invitations for bid (IFBs)
  - IFB is possible, but your requirements had better be rock solid and 100% defendable - that is not always easy to pair
- Piggybacking & Cooperative Contracts
  - Look carefully at the administrative fees charged by purchasing cooperatives and the terms and conditions
  - Some entities are simply not allowed to utilize this method for cloud-based purchases

General Considerations for all Cloud Types

- **Conducting background checks**
  - Anyone that has access to your data should be subject to background checks
  - Type of data determines the type of background check needed
- **Vetting resellers and 3rd parties**
  - Resellers and 3rd parties may be directly responsible for configuring features and tools that protect your data
  - They should have the skills and training required to ensure your data remains safe

Considerations Specific to Cloud Types

- Each cloud type has specific demands and roles on each party
- Failure to understand is the cause of most contract breaches
  - **IaaS:** You have the most control compared to the other types - the supplier is responsible for the physical security of servers while you are responsible for logical security of the servers
  - **PaaS:** You only control the application - the supplier takes responsibility over most services
  - **SaaS:** The supplier has most of the responsibility - therefore, you are placing all your faith in their hands
  - **XaaS:** This type of service can range from full GPS vehicle tracking systems to hardware as a service - therefore, you should view this as a sliding scale

Drafting Flexible Terms and Conditions

- With cloud, you are purchasing a fluid process rather than a static product
- With static features and terms and conditions, you end up with a product that cannot adapt
- Terms and conditions must allow for product adaptations as threats evolve and as your usage changes

Drafting Terms and Conditions – Defining Cloud Terms

- It is important to define what is needed in a procurement
  - Much of cloud is not based on industry standard definitions
  - A cloud supplier may view a term differently compared to the procuring entity
  - Some examples of terms you may want to define are Data, Data Mining, Data Breach, and Data Retention

Drafting Terms and Conditions – Disposal & Transfer

- You may wish to explore cryptographic erasure
  - This means encrypting a hard drive and then discarding the key
- You may want to or not want to purchase hardware at the end
  - What is the discounted rate at which the equipment will be purchased?
  - Should be negotiated into the contract
- How will disposal be different for single tenant versus a multi-tenant?
  - In single tenant, disposal is expensive but doable
  - In multi-tenant, may be complex or impossible to disentangle data

Drafting Terms and Conditions - Disentanglement

- Think about the next solution while preparing the first
  - Lock in a fixed cost for transitioning
  - Write terms and conditions that ensure the supplier will cooperate with any data transfer
  - Fix any consulting costs in place
  - Build in any application programming interface (API) or virtual private network (VPN) that will be needed to access data or transition data

Example disentanglement language: “Unless a cost is provided for services required to transfer data and customer data within this RFP response, then the service shall be provided at no charge.”

Functionality Matrix

- To create clear specifications, it may be helpful to utilize a functionality matrix
- It is sent to suppliers with the requirements already listed
- Suppliers then use the available code responses to determine how their product addresses your needs
- Typically, a supplier will meet some of your needs, need to incorporate some third-party software, and require some customizations

Functional Category: System-Wide

Available Response Codes

F	Provided fully functional out of the box or with configuration (no custom development)
CU	Customization/Software Enhancement (Any custom development)
TP	Third-party Software Required to Fully Provide Requirement (Third-party Software Must be Proposed
SR	Provided with Standard Report or Reporting Tool
CR	Custom Report Development Required
N	Not Included in this Proposal

Reference Number		Functional Requirements	Response	Module(s) Sub-Module(s) Required to Fulfill Requirements	Comments
		INTEGRATION AND ARCHITECTURE			
sw	1.00	System has fully integrated suites/modules/applications compliant with PCI, HIPAA, etc (If not integrated, please specify which modules are not integrated.	F		
sw	2.00	Software uses workflow to electronically route documents (and route/sore approvals across all:			
sw	3.00	Human Resources	F		
sw	4.00	Modules	F		
sw	5.00	Applications	F		
sw	6.00	System Toolsets are available for the following:			
sw	7.00	Workflow	F		
sw	8.00	Report writing	F		

Drafting Terms and Conditions – Outlining the Current Environment

- When outlining the current environment, include the following:
  - **All known integrations:** The integrations can be numerous - a lapse in security to one may be a threat to all
  - **All APIs:** List all applications that may transmit data to this system, then determine which of those sources will be required immediately and which at some future point
  - **Staff / personnel load from the customer side:** Think about how many end users you will have, and also consider the future

Drafting Terms and Conditions – Including Data Classification

- Earlier we discussed how a data classification tool can be used to assist end users in determining risk
  - Regardless if step was taken, the entity must review data and determine the impact to the entity if the data were breached
  - This data study must be done by the data owner who knows what is in the data and the laws surrounding the data

Drafting Terms and Conditions – Data Storage Types

- Consider the type of data storage needed
- For example:
  - **Hot storage:** Works best when needing instant access to data
  - **Cold storage:** Works best when needing monthly or less frequent access to data

Service Level Agreement (SLA)

- For SLA requirements, list what is acceptable for:
  - Up-time
  - Response time
  - Resolution time
  - Escalation factors
- Let us review each of these

Up-Time

- **Up-time** is the time that the system is available to the end user and fully functional
  - Most entities will negotiate for the highest level that can be afforded
    - 99% = 15 min per day 3.6 days per year
    - 99.9% = 1.5 min per day 8.75 hr. per year
    - 99.999% = 5.25 min per year
  - The entity can attempt to leverage damages against the supplier if these up-times are not maintained

Response Time & Resolution Time

- **Response time** is the time that is allowable for the supplier to acknowledge the call or ticket
  - Depending on the solution, some entities will negotiate an immediate response time
  - As the response time lengthens, the price usually drops
- **Resolution time** is the amount of time that the supplier has to resolve the problem once a call or ticket is received
  - One strategy for resolution time is to separate calls into categories
    - **Red:** This is critical functionality in the system
    - **Yellow:** This is urgent functionality in the system
    - **Green:** This is functionality that is important, but not critical or urgent

Escalation Factors

- **Escalation factors** outline how issues with the functionality or non-functionality of the system will be escalated by the supplier to achieve the SLA
  - If all factors are escalated to the highest level of resolution all the time, the price will be impacted

Method of Award

- Must be carefully crafted based on research
- Ensure all costs and options are included
- May includes services added during the contract period
- May want to lock hourly additional consulting service rates in place

Cloud Licensing

- Typically mirrors on premise software licensing
- Starts with identifying licensing type
  - Per seat, per named end user, etc.
- You need to see what that cost is to determine scalability and fairness of your financial award
- Watch as the contract evolves over time, cloud pricing changes
- Technical staff and procurement must be aware of the licensing structure and changes should be studied

Warranty, Maintenance & Support

- With cloud, all should be inclusive
- Should be included with any hardware that is part of the solution
- The supplier may push back or limit their responsibility to reduce liability
- There are different levels of support
  - Initially you need significant support
  - When the system undergoes upgrades, some services are needed
  - Only you can determine if the increased support will be worth the increased cost

Delivery Milestones

- Unlike software or hardware, you may have to pay immediately
- However, implementation services should be paid by deliverable milestone basis:
  - **10%:** Implementation plan that includes timeline, staffing plan, etc.
  - **10%:** Data conversion, which includes data migration and data cleanup
  - **10%:** Load testing
  - **10%:** End-user testing
  - **10%:** Training
  - **30%:** Go live
  - **20%:** 90 days burn-in period

Managing Costs

- By making the project deliverable-based you pay only when each portion of the project is completed
  - Each deliverable should have a fixed price
  - You can set the deliverable schedule in the terms and conditions or allow bidders to propose a schedule as part of their bid
  - Consulting is a high profit industry by nature, using a deliverable-based approach can help manage this cost

RFP Review

- Compare the RFP with the functionality matrix
- Every item in the matrix should be listed as a requirement
- A good strategy is to ask a third-party to peer review for you
- Consider a request for comment (RFC) if you have the time

Questions?

@NYS_OGS @NewYorkStateOGS #2022NYGovBuy

NEW YORK STATE OF OPPORTUNITY. NY GovBuy