NATIONAL 8(a) ASSOCIATION

ALASKA

REGIONAL CONFERENCE

JUNE 20-23, 2022 — ANCHORAGE

CMMC: CUI and Enclave Options

Ed Bassett, CISO, NeoSystems

NeoSystems®

Speaker

Ed Bassett

Chief Information Security Officer

NeoSystems

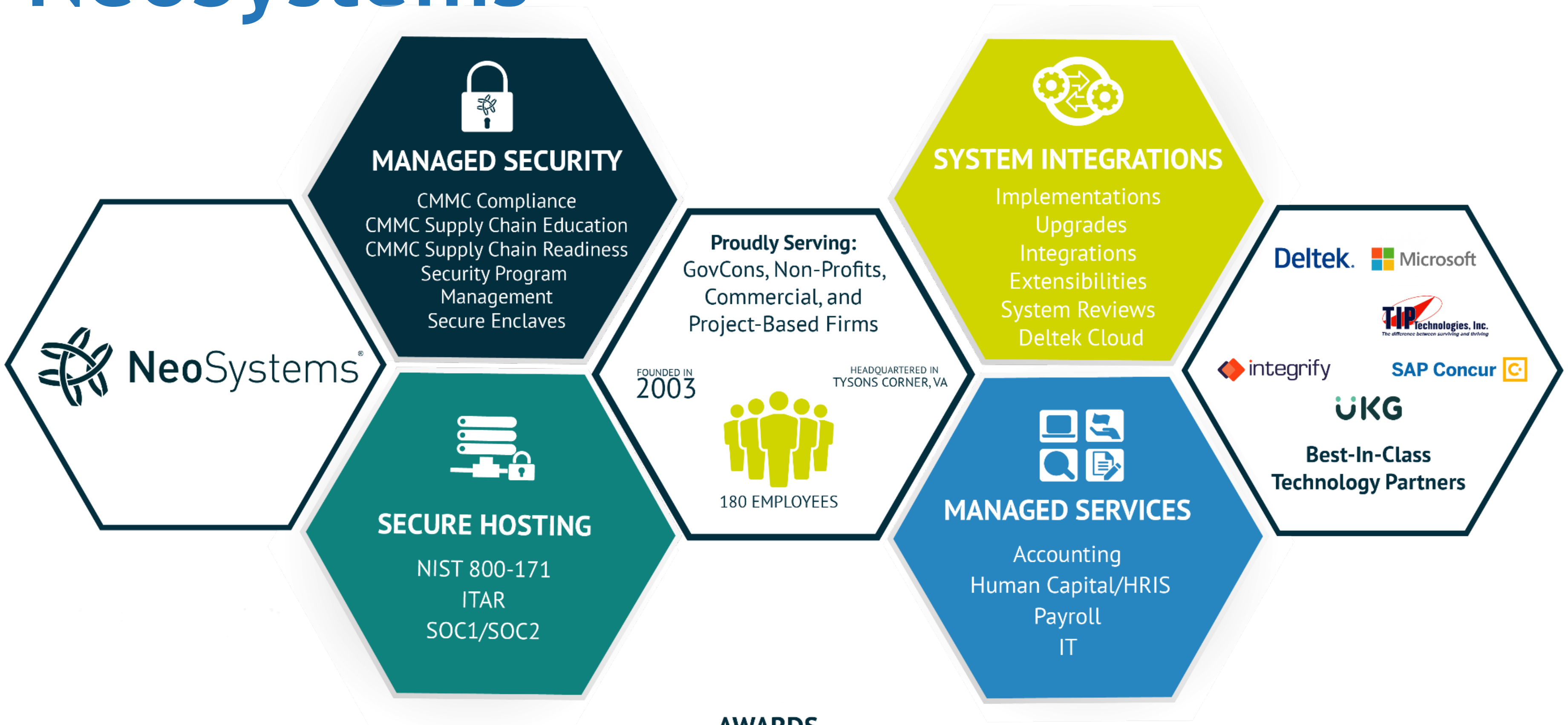
Agenda

Regulatory (and other) Expectations

4 Key Strategies for Small Businesses

What does “good” (enough) look like?

About NeoSystems



NeoSystems®

MANAGED SECURITY

CMMC Compliance
CMMC Supply Chain Education
CMMC Supply Chain Readiness
Security Program Management
Secure Enclaves

SECURE HOSTING

NIST 800-171
ITAR
SOC1/SOC2

Proudly Serving:
GovCons, Non-Profits, Commercial, and Project-Based Firms

FOUNDED IN 2003

HEADQUARTERED IN TYSONS CORNER, VA

180 EMPLOYEES

SYSTEM INTEGRATIONS

Implementations
Upgrades
Integrations
Extensibilities
System Reviews
Deltek Cloud

MANAGED SERVICES

Accounting
Human Capital/HRIS
Payroll
IT

Deltek. Microsoft TIP Technologies, Inc. integrify SAP Concur UKG

Best-In-Class Technology Partners

AWARDS

Inc. 5000 List for 7 Consecutive Years | SAP Concur Distinguished Partner Award
Adaptive Insights (Workday) Partner Momentum Award - Americas
Deltek Premier Partner Award: GovCon Consulting | E&Y Entrepreneur of the Year Finalist: Michael Tinsley

Why Cyber? Why Now?

Cost of Malicious Cyber activity on the U.S. economy: $57-109B/yr

Global cost of cybercrime: $600B/yr

Defense Industrial Base = 300,000+ companies

Inconsistent interpretation of requirements

Inconsistent implementation of cybersecurity

Target-rich environment for our adversaries

Problem: “Overreliance on ‘trust,’ in dealing with contractors, vendors, and service providers, has encouraged a compliance-oriented approach to security—doing just enough to meet the ‘minimum’ while doubting that sufficiency will ever be evaluated.”

Solution: “Structure acquisitions so contractors have a profit motive to enhance security.”

– Mitre, Deliver Uncompromised

Escalating Expectations

Government

- DFARS / NIST / FedRAMP
- CMMC (expect in contracts May 2023)
- SPRS reporting of assessment scores
- DIBCAC Audits
- CISA Shields Up

Primes

- Questionnaires
- SPRS
- Contractual flow downs

Insurance

- Minimum requirements to obtain coverage

Banking

- Part of underwriting evaluation process

Challenges for Small Business

Same requirements as large contractors

Strong enforcement by gov’t and primes

Esoteric technical requirements

Offerings from major IT and cloud providers not compliant by default

Compliant practices not offered by many MSPs

May require IT transformation

- New cloud environment
- System rebuilds

Ongoing operational processes

4 Key Strategies for Small Businesses

#1 Manage Scope

#2 Manage Operational Cost

#3 Shift the Compliance Burden

#4 Manage Supply Chain Risk

NeoSystems®

NATIONAL 8(a) ASSOCIATION®

Key Strategy #1

Manage Scope

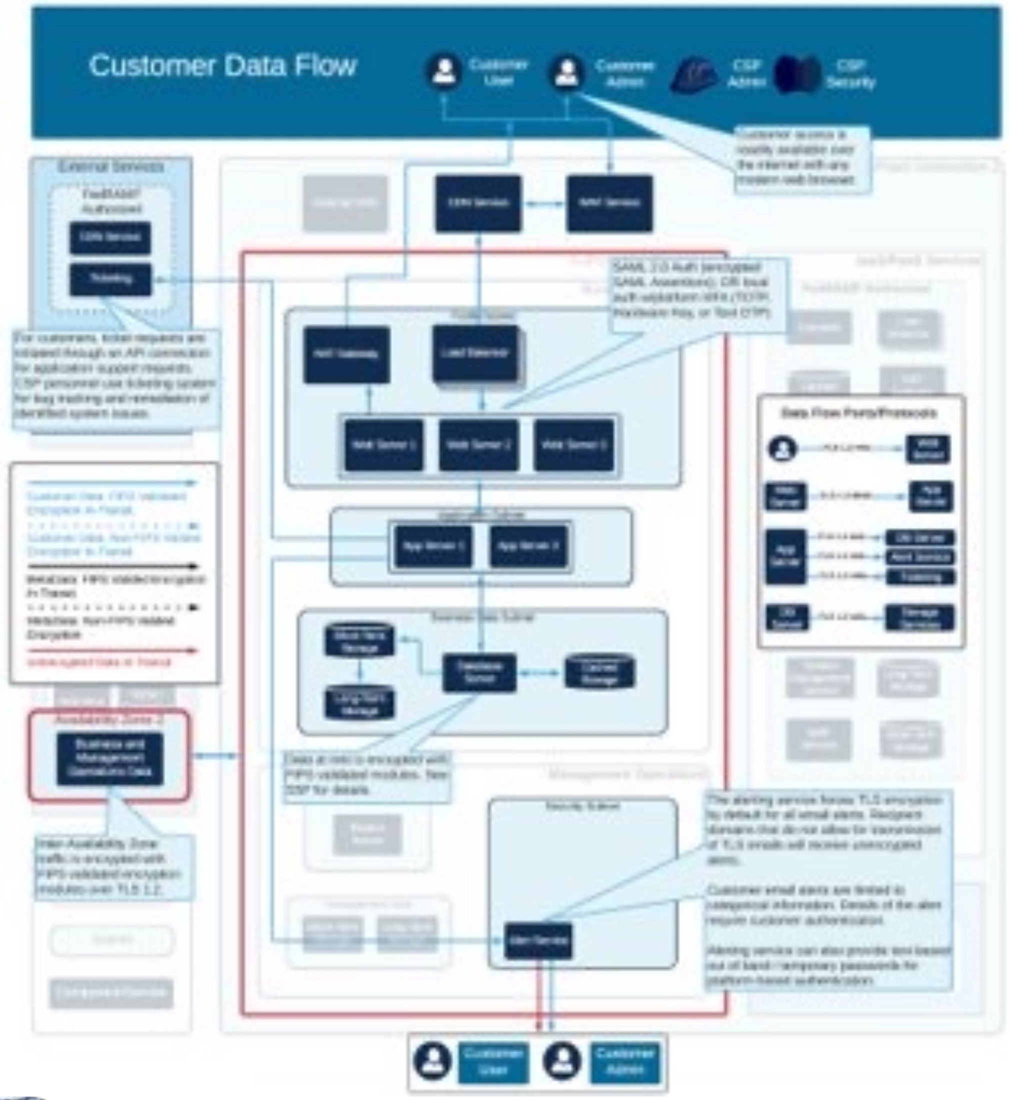
Mapping Data Flows

CMMC is designed to enhance the protection of controlled unclassified information (CUI) and Federal Contract Information (FCI) in the DoD supply chain

Nearly all contractors possess FCI

Identifying CUI can be challenging

Key decision point: which systems will be capable of storing and processing CUI



FCI versus CUI

What FCI is:

- Not intended for public release
- Provided by the government under a contract to develop or deliver a product or service to the government
- Generated for the government under a contract to develop or deliver a product or service to the government

What FCI isn't:

- Not including information provided by the government to the public such as a public website
- Simple transactional information, such as necessary to process payments

CUI ≠ Level 1

- If you handle CUI, Level 1 will not be enough
- CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls

Any organization that possesses Federal Contract Information (FCI) as defined in FAR 52.204-21 will need to meet CMMC Level 1.

Best Practices For Identifying CUI

Inventory all existing contracts

Focus on contracts where CUI may be potentially involved

- DoD, DHS, DoE
- Identify “high risk” contracts

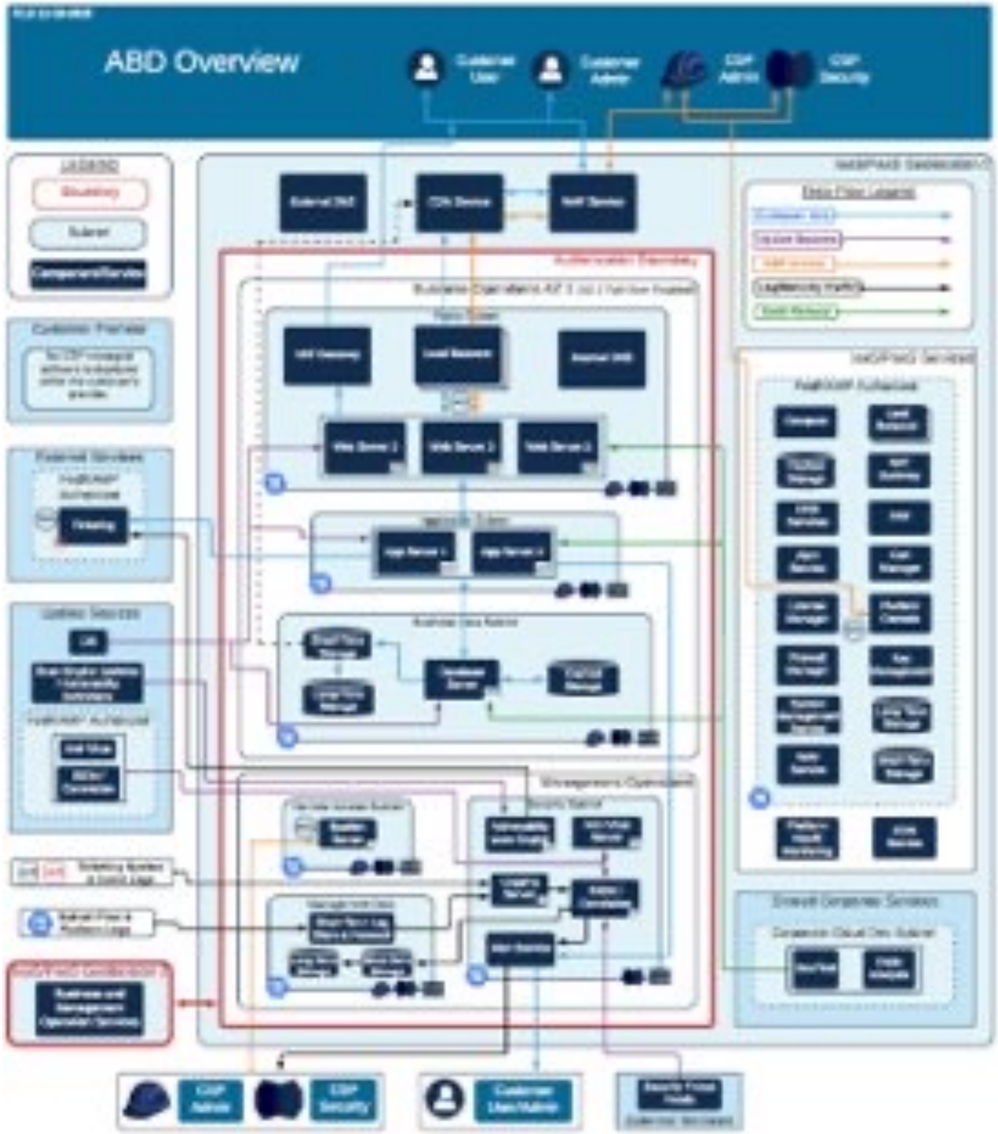
Review solicitations for current bid/proposal efforts

Consider prime-sub relationships

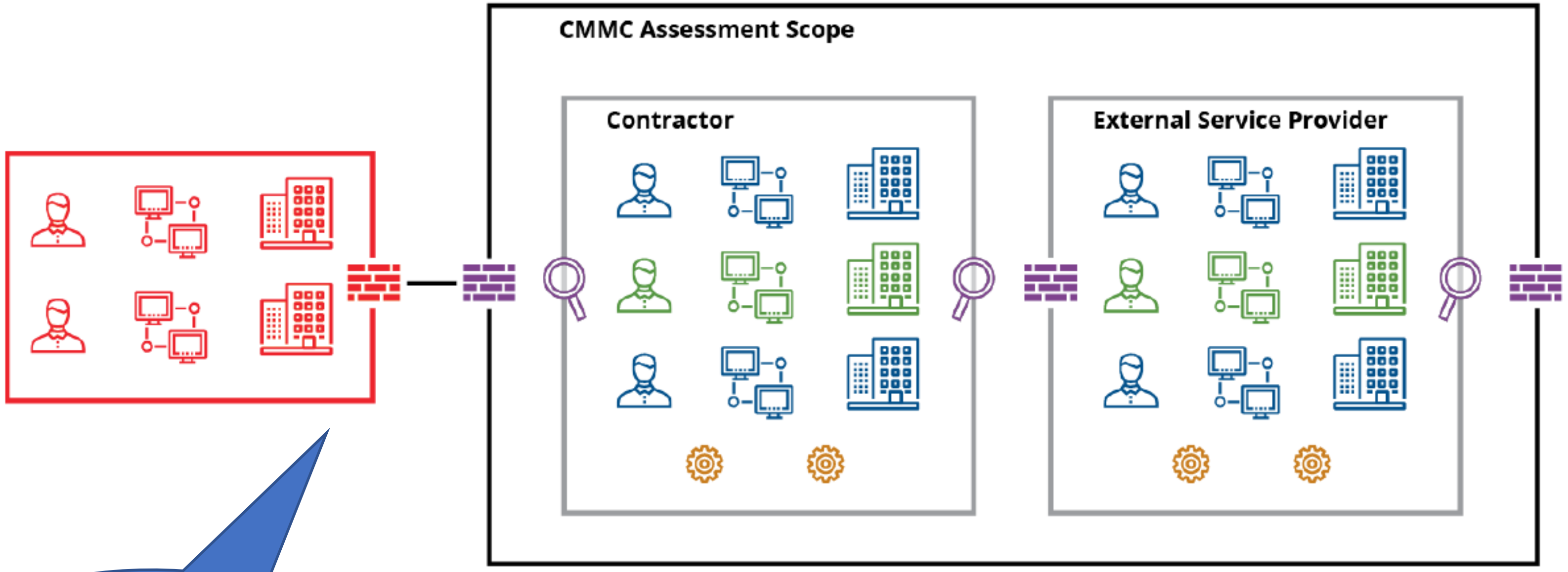
Scope and Boundary

- Follow the data
- Segmentation
- Enclave approaches
- Cloud systems
- External connections
  - Service providers
  - Customers/Suppliers

The Organization Seeking Certification must establish their system boundary. This will define the scope of the CMMC certification assessment.



Segmentation of Networks and Systems



🟦 CUI Assets
🟪 Security Protection Assets
🟩 Contractor Risk Managed Assets
🟧 Specialized Assets
🟥 Out-of-Scope Assets

"Out-of-Scope" requires physical or logical separation

Without adequate segmentation, the entire enterprise environment will be "in scope".

Source: CMMC Assessment Scope, Level 2
https://www.acq.osd.mil/cmmc/docs/Scope_Level2_V2.0_FINAL_20211203.pdf

Scope

Level 1 Assessment covers:

- FCI Assets (process, store, or transmit)

Level 2 Assessment covers:

- CUI Assets
- Security Protection Assets
- Contractor Risk Managed Assets
- Specialized Assets

Out-of-Scope Assets require approved “separation techniques”:

- Logical separation (e.g., firewalls, VLANs)
- Physical separation (e.g., gates, locks, badge access, guards)

Enclaving

Isolated virtual work environment built and maintained to Federal cybersecurity standards

Powerful scope and cost control technique

Consider whether federal data can be sequestered:

- Separate users or
- Separate systems

Pros:

- Existing corporate systems out of scope
- Reduced exposure to threats
- Easy for users to understand
- Quick to implement

Cons:

- Must segregate users and/or data
- Duplicate productivity environments
- More difficult to communicate across platforms
- Potential for data leakage

Common Scope Scenarios

Single Environment	FCI and CUI (Level 2)	
Separate CUI Environment	FCI (Level 1)	CUI (Level 2)
Out-of-Scope Corporate	Non-Federal (Out-of-Scope)	FCI and CUI (Level 2)

Why Enclaves

Reduce footprint - Minimize the in-scope area for audit and compliance

Reduce exposure to threats

Minimize disruption to existing IT infrastructure

“Purpose-built” for compliance

Shorten time to CMMC certification

Start small and scale up as needs grow

Sequester the data – Users come to the data; not bringing data to the User

Enforce Zero-Trust

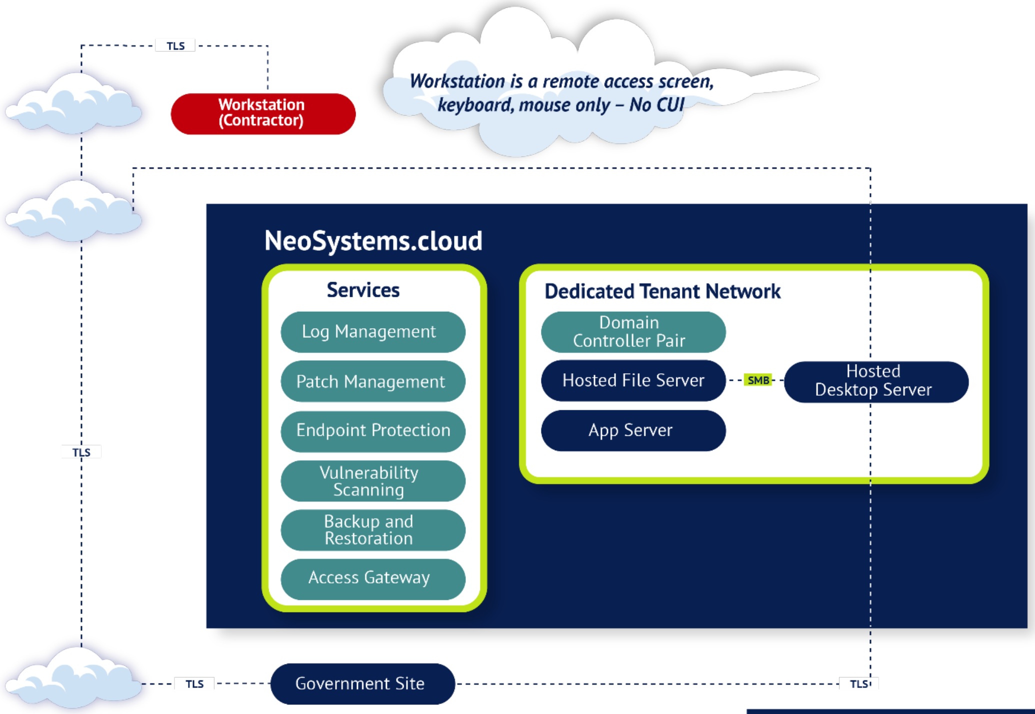
Example Enclave - Basic

Basic Use Enclave

- Virtual desktop workspace
- File Storage
- Web Browser Access

Options/Add-ons

- Desktop Apps
- Enterprise Apps (BYOL)

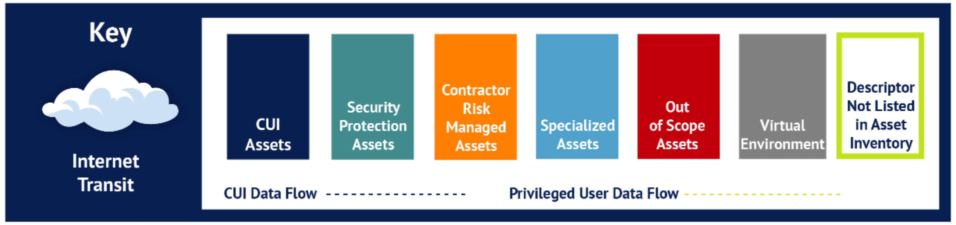


BASIC ENCLAVE

- Supports NIST 800-171, DFARS 252.204-7012, and CMMC requirements
- Sequesters CUI and ITAR data
- Allows authorized end-users to process, store, and transmit CUI/CDI inside enclave
- Supports Cloud based apps
- Health & Availability Monitoring

ADD HOSTED APPS

- Add dedicated VMs to host applications managed by Neo
- SQL databases available
- BYOL



Key
Internet Transit
CUI Assets
Security Protection Assets
Contractor Risk Managed Assets
Specialized Assets
Out of Scope Assets
Virtual Environment
Descriptor Not Listed in Asset Inventory
CUI Data Flow
Privileged User Data Flow

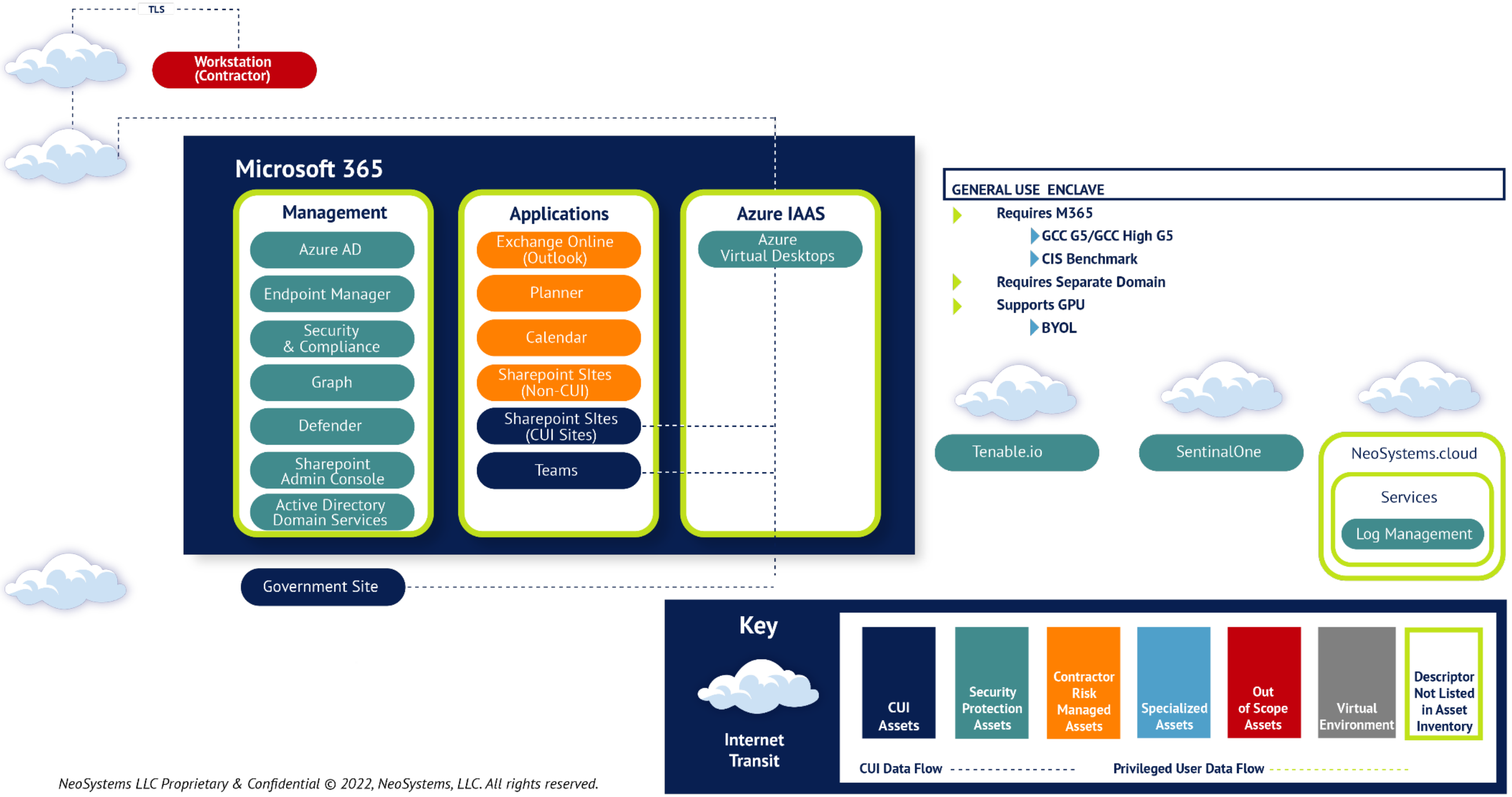
Example Enclave - Full Featured

Full Featured Environment

- Virtual desktop workspace
- Microsoft 365, including collaboration tools
- Outlook Email
- Web Browser Access

Options/Add-ons

- Graphics-intensive Desktop Apps requiring GPU (BYOL)
- Enterprise Apps (BYOL)



TLS

Workstation (Contractor)

Microsoft 365

Management
- Azure AD
- Endpoint Manager
- Security & Compliance
- Graph
- Defender
- Sharepoint Admin Console
- Active Directory Domain Services

Applications
- Exchange Online (Outlook)
- Planner
- Calendar
- Sharepoint SItes (Non-CUI)
- Sharepoint SItes (CUI Sites)
- Teams

Azure IAAS
- Azure Virtual Desktops

Government Site

GENERAL USE ENCLAVE
- Requires M365
  - GCC G5/GCC High G5
  - CIS Benchmark
- Requires Separate Domain
- Supports GPU
  - BYOL

Tenable.io

SentinalOne

NeoSystems.cloud

Services

Log Management

Key

Internet Transit

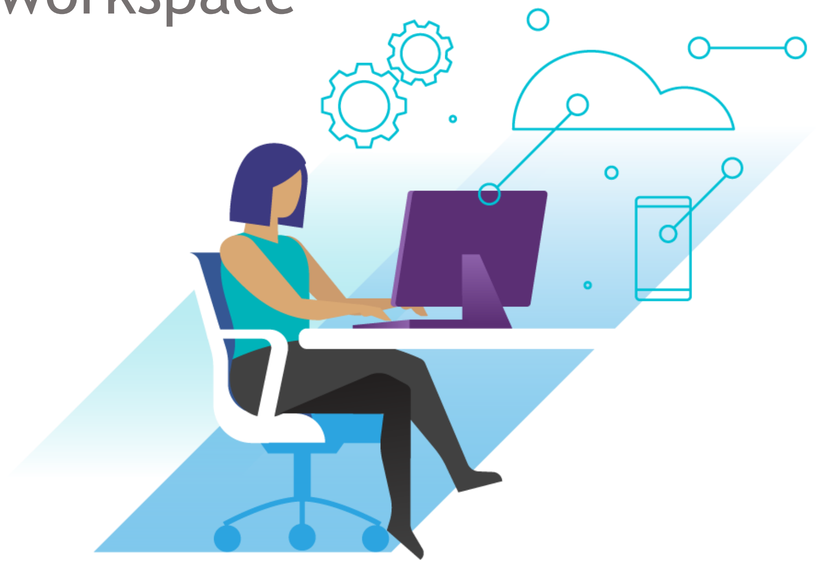
CUI Assets	Security Protection Assets	Contractor Risk Managed Assets	Specialized Assets	Out of Scope Assets	Virtual Environment	Descriptor Not Listed in Asset Inventory

CUI Data Flow ----------------

Privileged User Data Flow ----------------

Enclave User Experience

May be an everyday workspace or special-purpose workspace



Use your own laptop

- Web browser access from anywhere
- Individual user account to login
- Multifactor authentication using an app on phone

Full Windows Desktop experience

- Most commercially available software supported

Store Files

- Persistent desktop allows user to save files to usual places (Desktop, Documents, etc.)
- File share – can have separate security groups - everyone in a group can see files for that security group

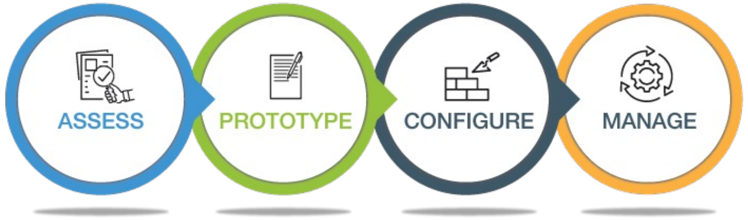
Move data in/out of enclave using web services

- Option for EFT/SFTP service
- Option for M365 Outlook attachments

Key Strategy #2

Manage Operational Cost

CMMC Approach



ASSESS

1. Determine scope, boundary, and CUI data flows for the CMMC environment
2. Evaluate corporate security policies
3. Evaluate IT use cases and current environment
4. Complete Security Control Matrix

PROTOTYPE

1. Select best-fit reference architecture
2. Identify any needed modifications
3. Set up prototype

CONFIGURE

1. Complete system security plan and supporting security program documentation
2. Complete production IT build-out
3. Migrate users and data
4. Train users

MANAGE

1. Continuous monitoring
2. Capacity/performance monitoring
3. Vulnerability/patch mgmt.
4. Change mgmt.
5. User support
6. Break-fix
7. Audit readiness/support
8. Security governance

Cloud + Managed Services

Cloud services must be FedRAMP Moderate equivalent

Cloud provider responsible for security of the infrastructure

Still many security hardening settings required (e.g., CIS Benchmark)

Add-on managed services:

- Initial build of cloud tenant environment
- Hardening and security configuration
- Configuration management and change control
- Updates as threats and requirement change
- User administration and support
- Application support
- Patch management
- Log management
- Data backup
- Continuous monitoring of compliance
- Evidence of compliance for audit (CMMC or DIBCAC)
- Supporting policy, procedures, training
- Alert monitoring and investigation
- Incident response and reporting

Security Program Controls

✓

- **Responsibility for cybersecurity compliance**, before, during, and after the CMMC audit.
- **Information Security Officer (ISO)** - "go-to" person for all security compliance items and is responsible to drive the security program from beginning to end.

1X

- **Gap assessment** mapped directly to the applicable compliance requirements (CMMC, FAR, DFARS, etc.)
- Define CMMC **boundaries and data flows** to establish the **scope** of certification.
- **Foundational documents** needed for a mature security program – policies, procedures, security plans, etc.

- **On-going support** to drive periodic recurring security program **continuous monitoring** tasks on a strict schedule, ensuring that all required processes operate effectively.
- **Review** data from system **activity logs, vulnerability scans**, and open **security roadmap** items monthly to tune alerts and prioritize actions.

- Access to **security expertise** for questions, new systems, new risks, etc.

Key Strategy #3

Shift the Compliance Burden

Selecting Solutions

For any CMMC level above Level 1, consider a specialized security services provider who can provide:

- Accelerated process maturity
- Access to specialized skillsets
- Turnkey technical solutions

Evaluate technology partner and service provider commitment to meeting CMMC requirements

Use cloud services and managed services to shift portions of the compliance burden

Adopt standardized solutions:

- Technical components
- Operational services

Utilizing Service Providers

Overlaying CMMC controls on existing IT may not be the best way

- Retrofit vs re-build
- End-of-life-systems – isolate and separately manage

Cloud adoption

- Cloud-only vs hybrid designs
- FedRAMP vs CMMC
- Not all cloud providers are created equal
- All claim to be “secure”
- Many are FedRAMP
- Shared responsibility models and CMMC alignment vary greatly

Service Providers

- Scoping guidance brings security tools into scope
- Access to data must be considered

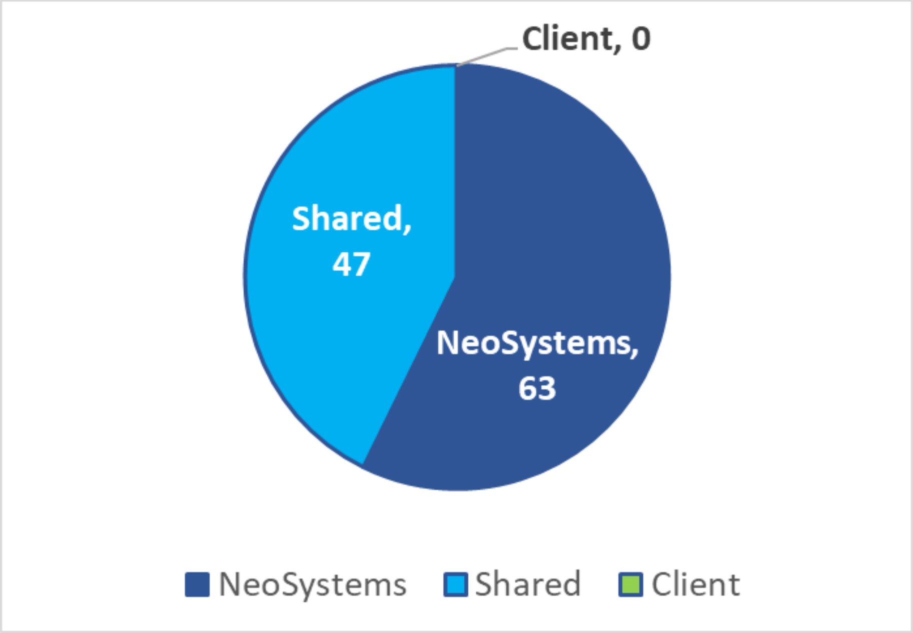
Shared Responsibility Model

Example shows the allocation of the 110 CMMC Level 2 controls for a Cloud + Managed Services arrangement

Client responsibilities can vary greatly

Inheritance for CMMC assessment still being worked out by DoD

For now, rely on contractual commitment to specific shared responsibilities



Key Strategy #4

Manage Supply Chain Risk

Next Steps for Contractors

Review contracts – what level will you need?

Prepare for certification: invest in systems and people. This is a Go/No-Go

Review contracts for current cybersecurity requirements. Remember, the DFARS 7012 clause requires compliance with 110 security controls and reporting breaches within 72 hours

Examine incident reporting framework

- What cyber threats are being tracked?
- What “incidents” are being reported? When?
- What information is being collected? How is it being preserved?

Strategies for Subcontractors

Draft subcontract agreements that require CMMC certifications and DFARS requirements. This includes -7012 and -7019 and -7020.

Allow for unilateral changes when the Government passes on a change.

Require subcontractors comply with cybersecurity investigations.

Permit termination if subcontractors do not comply with cybersecurity requirements.

Smallest companies are most at risk.

Do not forget about independent contractors.

What does “good” (enough) look like?

Achieving effective security and demonstrating compliance

“M” is for Maturity

What is Known About Certification

Assessments are conducted as a self-assessment, an independent C3PAO, or the Government

Type of assessment depends on level required

C3PAOs are authorized by the Cyber AB

Assessment teams led by a Certified Assessor (CA)

The assessment criteria (“the test”) is well defined

- CMMC Model
  - https://www.acq.osd.mil/cmmc/docs/ModelOverview_V2.0_FINAL2_20211203.pdf
- Level 1 Self-Assessment Guide
  - https://www.acq.osd.mil/cmmc/docs/AG_Level1_V2.0_Final_20211210.pdf
- Level 2 Assessment Guide
  - https://www.acq.osd.mil/cmmc/docs/AG_Level2_MasterV2.0_FINAL_202112016.pdf

Scope of Certification

Contractors are required to establish the scope of their subsequent certification

Can achieve a specific CMMC level for their entire enterprise network or for specific segment(s) or enclave(s), depending on where the information to be protected is handled and stored: CMMC follows the data

CMMC assessment will look at practices that apply to the system(s) designated for handling and storing of Federal Contract Information (FCI), Controlled Unclassified Information (CUI), or other controlled data types

Out-of-Scope systems will not be assessed

Security tools and service provider systems will be evaluated, even if they do not store and process federal data directly.

Scope is determined based on FCI/CUI location and target CMMC Level certification

Assessment Vs Self Attestation

Assessment methods

- Interview – hold discussions with individuals or groups
- Examine – review, inspect, observe, study, or analyze assessment objects
- Test – exercising assessment objects to compare actual vs expected behavior.

Assessments involve 2 of the 3 assessment methods and corroborating evidence for each control requirement

C3PAO determines assessment objects with Contractor during planning

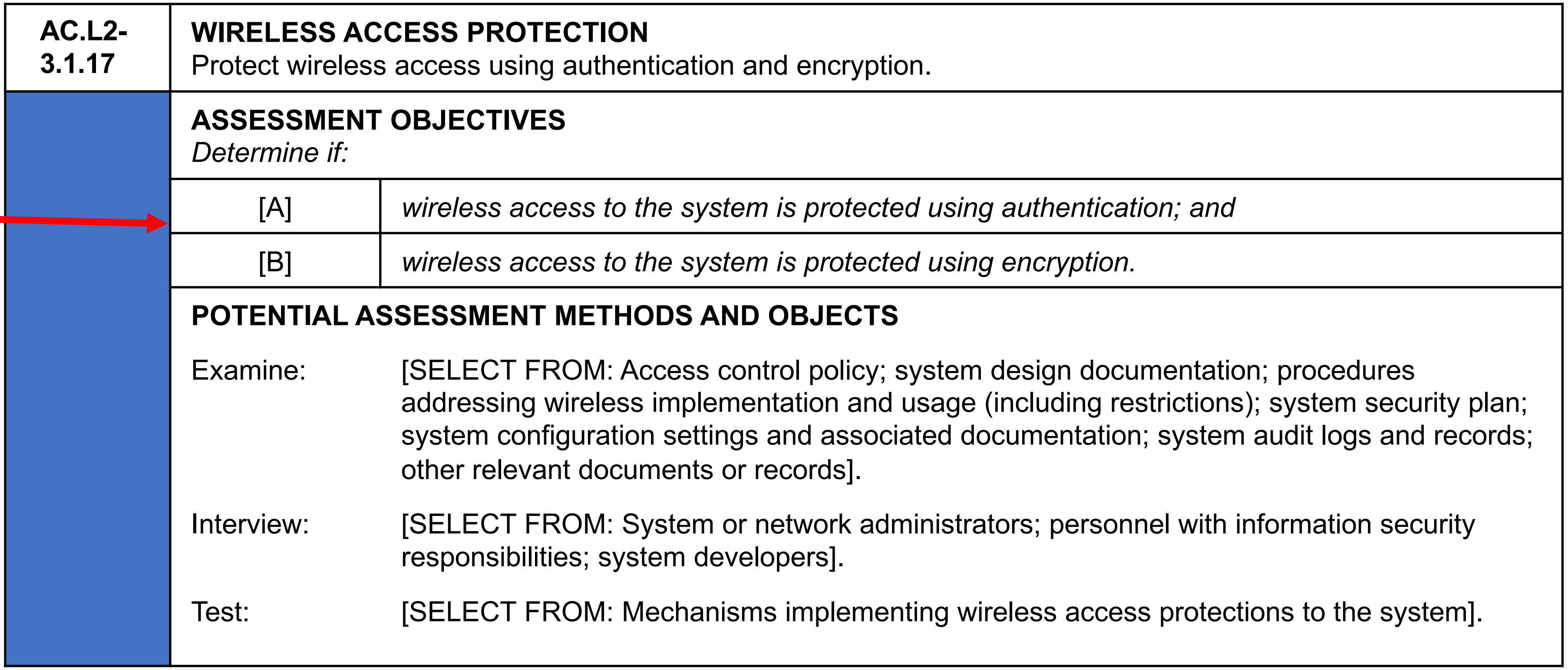
C3PAO determines the assessment methods for each control requirement

Key Concepts

- Adequacy
- Sufficiency

Control Requirement Example

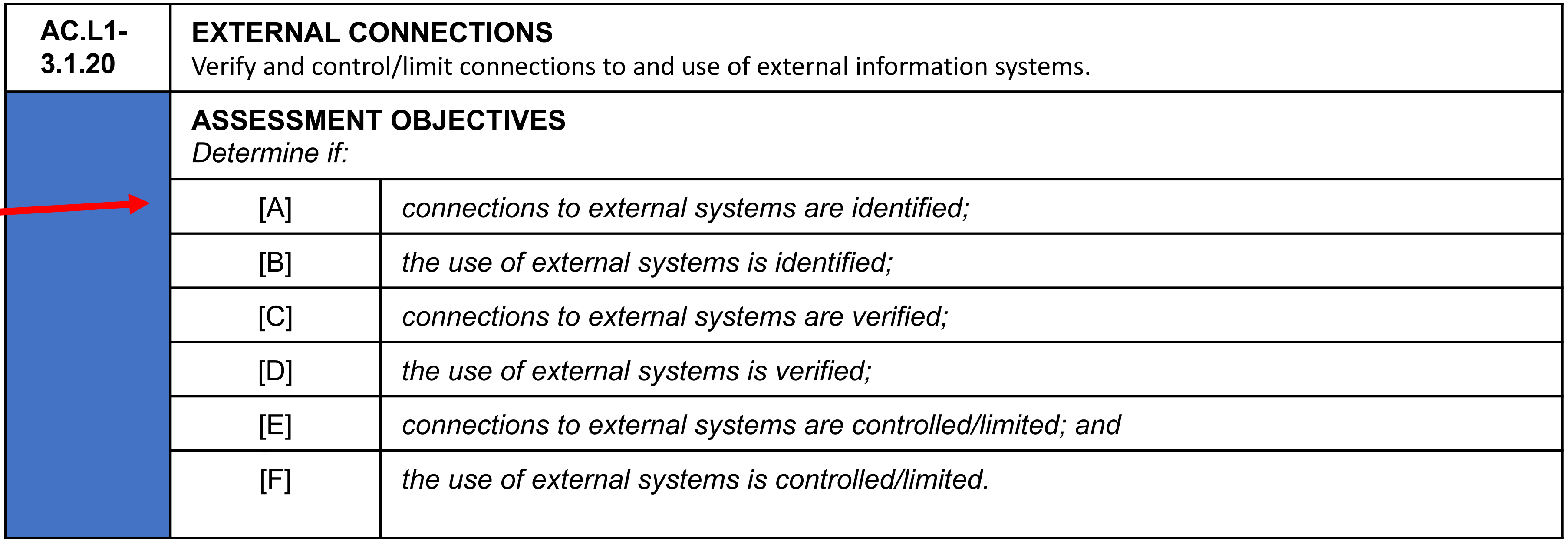
Must meet All Objectives



AC.L2-3.1.17	**WIRELESS ACCESS PROTECTION** Protect wireless access using authentication and encryption.	
	ASSESSMENT OBJECTIVES *Determine if:*	
	[A]	*wireless access to the system is protected using authentication; and*
	[B]	*wireless access to the system is protected using encryption.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS	
	Examine:	[SELECT FROM: Access control policy; system design documentation; procedures addressing wireless implementation and usage (including restrictions); system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].
	Interview:	[SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].
	Test:	[SELECT FROM: Mechanisms implementing wireless access protections to the system].

Another Example

Must meet All Objectives



AC.L1-3.1.20	**EXTERNAL CONNECTIONS** Verify and control/limit connections to and use of external information systems.	
	ASSESSMENT OBJECTIVES *Determine if:*	
	[A]	*connections to external systems are identified;*
	[B]	*the use of external systems is identified;*
	[C]	*connections to external systems are verified;*
	[D]	*the use of external systems is verified;*
	[E]	*connections to external systems are controlled/limited; and*
	[F]	*the use of external systems is controlled/limited.*

Design Controls

Identification of Controls

- Who - Control Owners (Internal and External) that will be “Interviewed”
- How – manual, automated, IT-dependent manual
  - Measured?
- When – what frequency

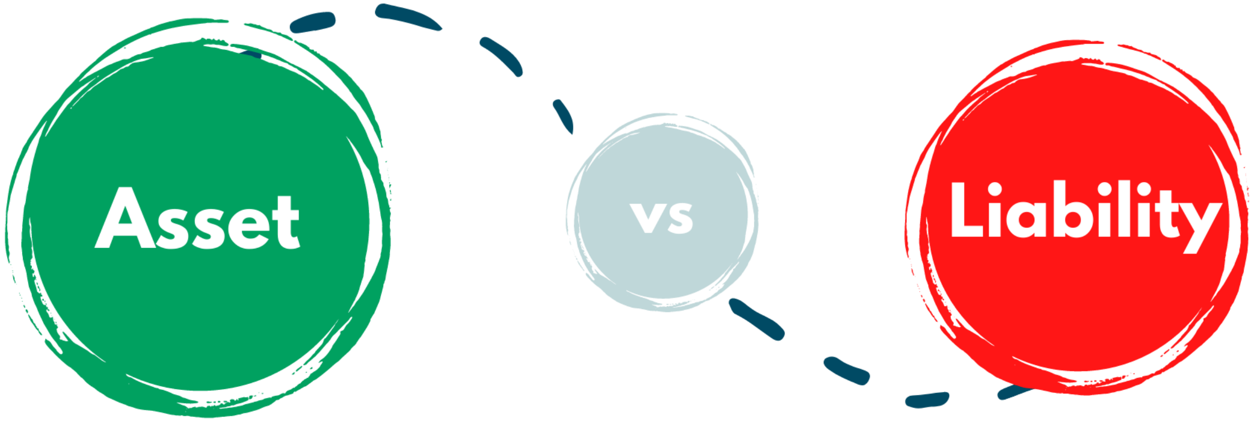
Evidence Collection (“2 Pieces of Corroborating Evidence”)

- Policies & Procedures, Forms, etc.
- System generated – configuration settings, logs, etc.
- Build history of operational performance

Documentation of Environment

- SSP & Data Flow
- POA&M

What’s Your Cyber Risk?



Asset

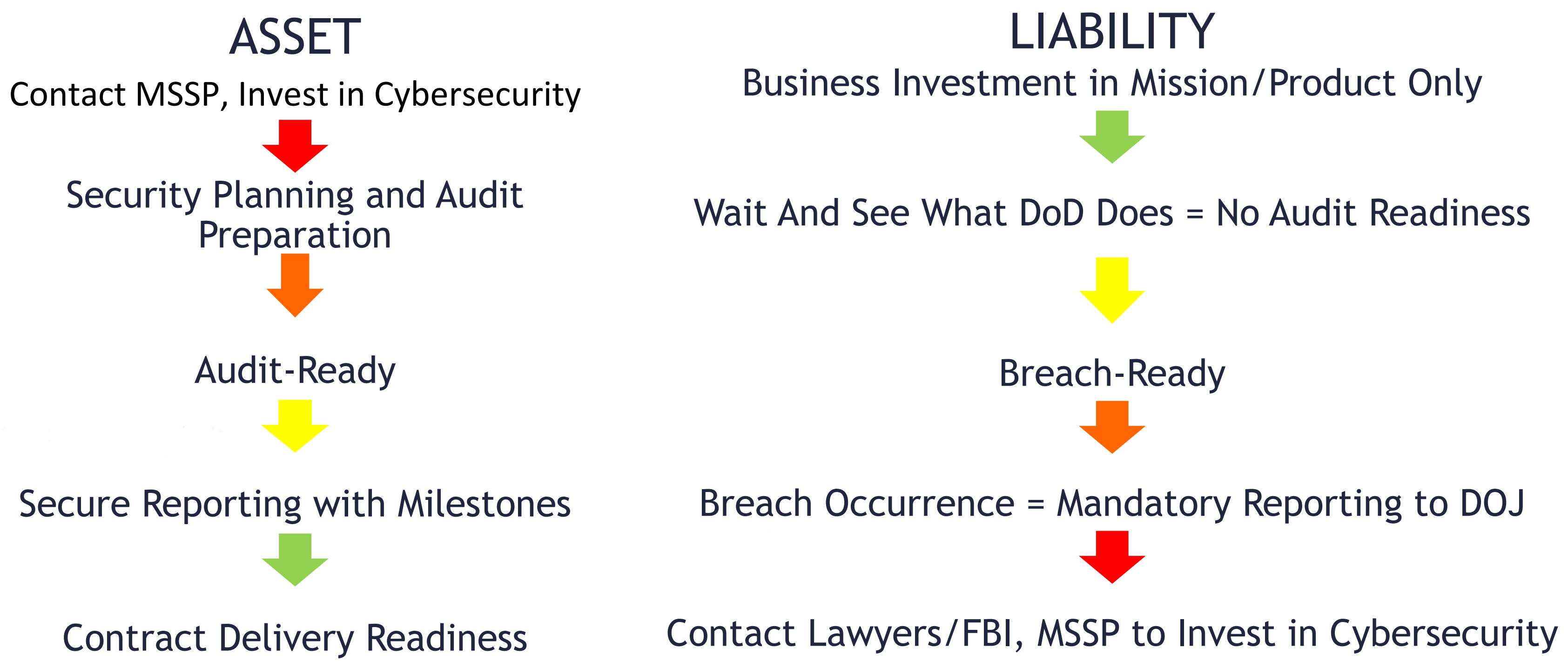
vs

Liability

Secure, Compliant, Contract-Ready

What’s Your Cyber Risk?

Which End Are You On?



ASSET

Contact MSSP, Invest in Cybersecurity

↓

Security Planning and Audit Preparation

↓

Audit-Ready

↓

Secure Reporting with Milestones

↓

Contract Delivery Readiness

LIABILITY

Business Investment in Mission/Product Only

↓

Wait And See What DoD Does = No Audit Readiness

↓

Breach-Ready

↓

Breach Occurrence = Mandatory Reporting to DOJ

↓

Contact Lawyers/FBI, MSSP to Invest in Cybersecurity

For PRIMES

Who is an ASSET or a LIABILITY in your Supply Chain?

IN THE END IT COMES DOWN TO BUSINESS RISK

- The responsibility of Primes is to ensure readiness for primes AND subs
- Be in a competitive position to fully deliver on compliance requirements
- Prepare for future contracts and be in a competitive position to bid
- Look at sole-source contracts that may be in jeopardy
- Have peace of mind with small business compliance (NIST SP 800-171 + CMMC)
- Government-wide agency adoption of cybersecurity standards

It's just good cyber hygiene that mitigates risking contracts and business!

For SUBS

Is your Business an Asset or a Liability to your PRIME?

IN THE END IT COMES DOWN TO BUSINESS RISK

- The responsibility of Subs is to ensure cyber hygiene and mitigate risk
- Deliver value upwards and ensure long-term competitive advantage
- Prepare for future contracts
- Solidify position to adhere to additional/future compliance requirements
- Provide peace of mind beyond your current contracts
- Government-wide agency adoption of cybersecurity standards
- Demonstrate cyber capability in a competitive market

It’s just good cyber hygiene that mitigates risking contracts and business!

Learn more about CMMC and Cybersecurity Compliance

On-Demand Webinars and Podcasts

- www.neosystemscorp.com

Join our Cybersecurity Town Halls alternate Wednesdays at 1pm EDT (9am AKDT) or on-demand

- Visit our website to register

Contact Information

Ed Bassett

Ed.bassett@neosystemscorp.com

571-234-5094

www.neosystemscorp.com

NATIONAL 8(a) ASSOCIATION

NeoSystems®