ASSESSING RISK OF OUTSOURCING THE CROWN JEWELS

Talk Summary

- What are Outsourced Network Services?
- Expanding Use of Outsourced Network Services
- Industry/Government/Academic Effort to Address Risks due to Outsourcing Network Services
- Conceptual Outline of Outsourcing Network Services Assessment Tool (ONSAT) prototype to assist in making risk management decisions when outsourcing network services

Outsourced Network Services

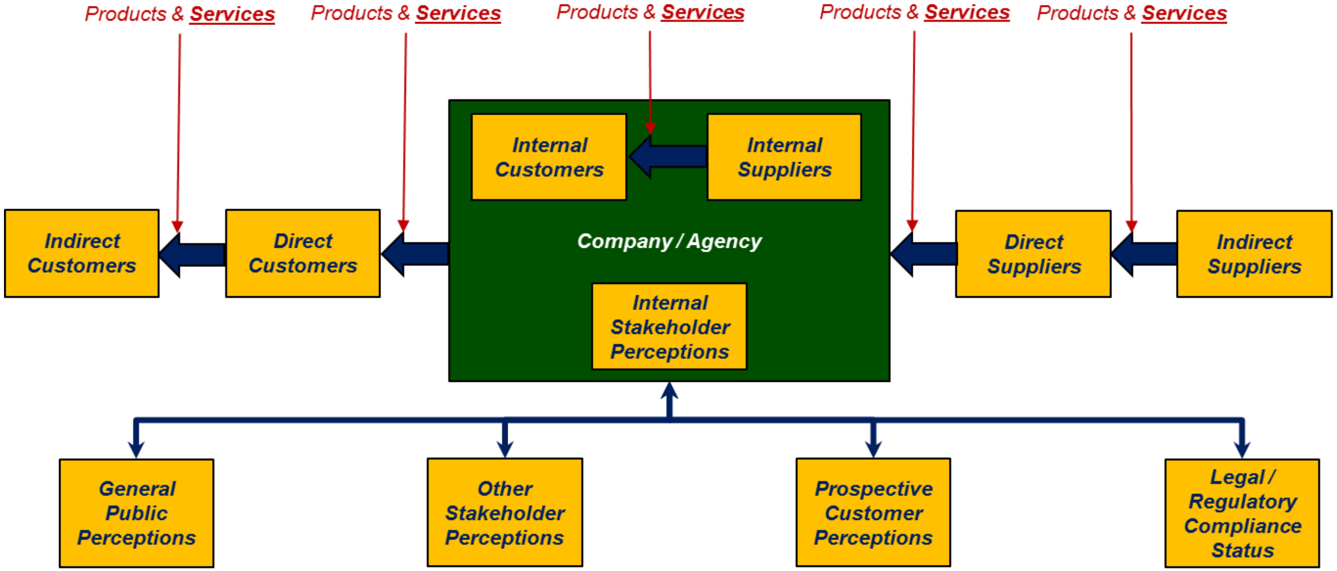
Definition:

- 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.

Expanding Use of Outsourced Network Services

- Often it is cost-effective to outsource Information and Communication Technology (ICT) Services.
  - Infrastructure
  - Maintenance and Support
  - Security and Incident Response
  - Business Services

What Are We Worried About?



Products & Services

Products & Services

Products & Services

Products & Services

Products & Services

Internal Customers

Internal Suppliers

Indirect Customers

Direct Customers

Company / Agency

Direct Suppliers

Indirect Suppliers

Internal Stakeholder Perceptions

General Public Perceptions

Other Stakeholder Perceptions

Prospective Customer Perceptions

Legal / Regulatory Compliance Status

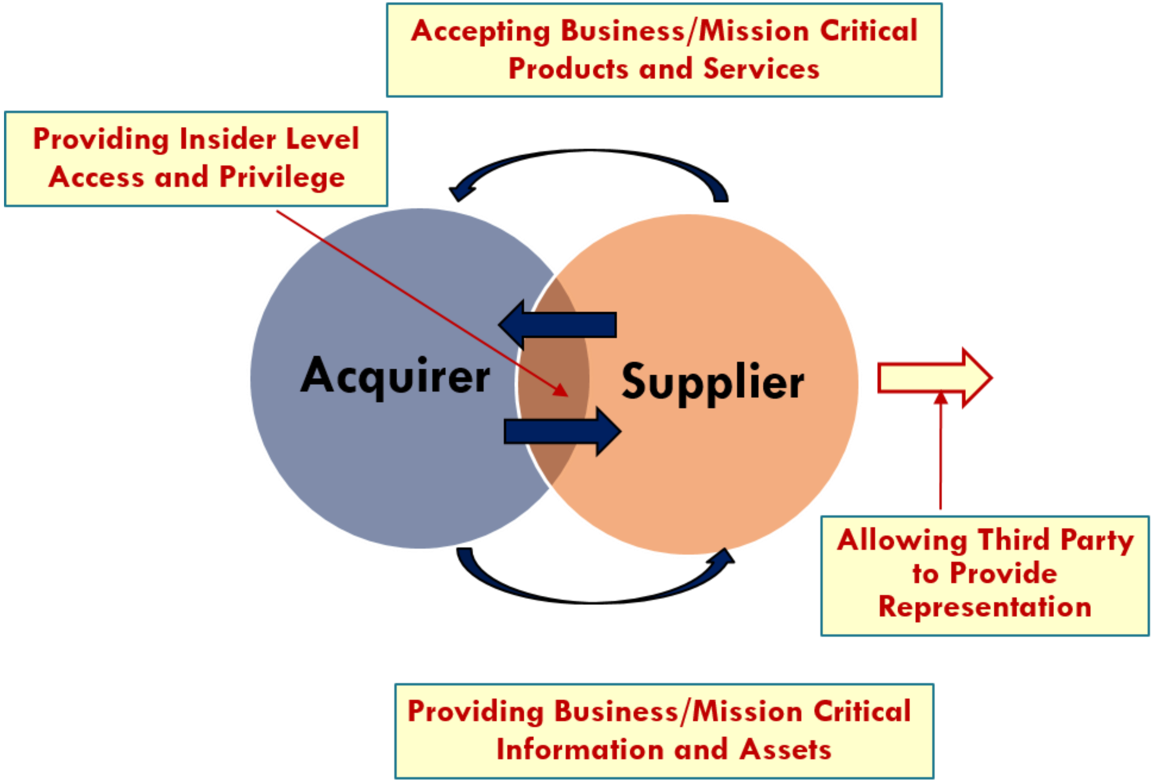
Potential Direct Harmful Consequences of Inferior / Subverted Products and Services

- Degraded / Subverted Products & Services
- Degraded / Subverted Operations & Processes
- Degraded / Subverted / Compromised Business/Mission Critical Information
- Degraded / Subverted / Compromised Customer Entrusted Information
- Degraded / Subverted Business/Mission Critical Assets
- Degraded / Lost Business/Mission Critical Resources
- Degraded / Lost Business/Mission Critical Partnerships
- Degraded Business/Mission Critical Reputation
- Degraded Legal / Regulatory Compliance Status

Potential Indirect Harmful Consequences of Inferior / Subverted Products and Services

- Lost Business (Long Term)
- Lost Mission Authority
- Degraded Critical National Infrastructure
- Degraded National Security

Expanding Boundaries of Enterprise to Partner


Accepting Business/Mission Critical Products and Services
Providing Insider Level Access and Privilege
Acquirer
Supplier
Allowing Third Party to Provide Representation
Providing Business/Mission Critical Information and Assets

- *Protect Integrity and Quality of Supplied Products and Services*
- *Protect Provided Access and Privilege (Personnel/ Electronic)*
- *Protect Confidentiality, Integrity, Authentication, Non-repudiation, and Availability of Information and Assets*
- *Protect Integrity of Reputation*

Outsourced Service Trust Relationships
between Acquirer and Supplier

Business Care Abouts	Security Problem Space Issues
□ Protect Provided Access and Privilege (Personnel / Electronic)	□ Providing Insider Level Access and Privilege ◘ Similar to Insider Concerns
□ Protect Integrity and Quality of Supplied Products and Services	□ Accepting Business/Mission Critical Products and Services ◘ Entrusting Third Party with Integrity of Processes and Products ◘ Similar to HW/SW Supply Chain Concerns
□ Protect Confidentiality, Integrity, Authentication, Non-repudiation, and Availability of Information and Assets	□ Providing Business/Mission Critical Information and Assets ◘ Entrusting Third Party to Protect Mission Critical Confidentiality and Value ◘ Similar to Information Assurance, Physical Security, and Insider Concerns
□ Protect Integrity of Reputation	□ Allowing Third Party to Provide Representation ◘ Entrusting Third Party to Project Reputation

Industry, Academia, and Government Effort

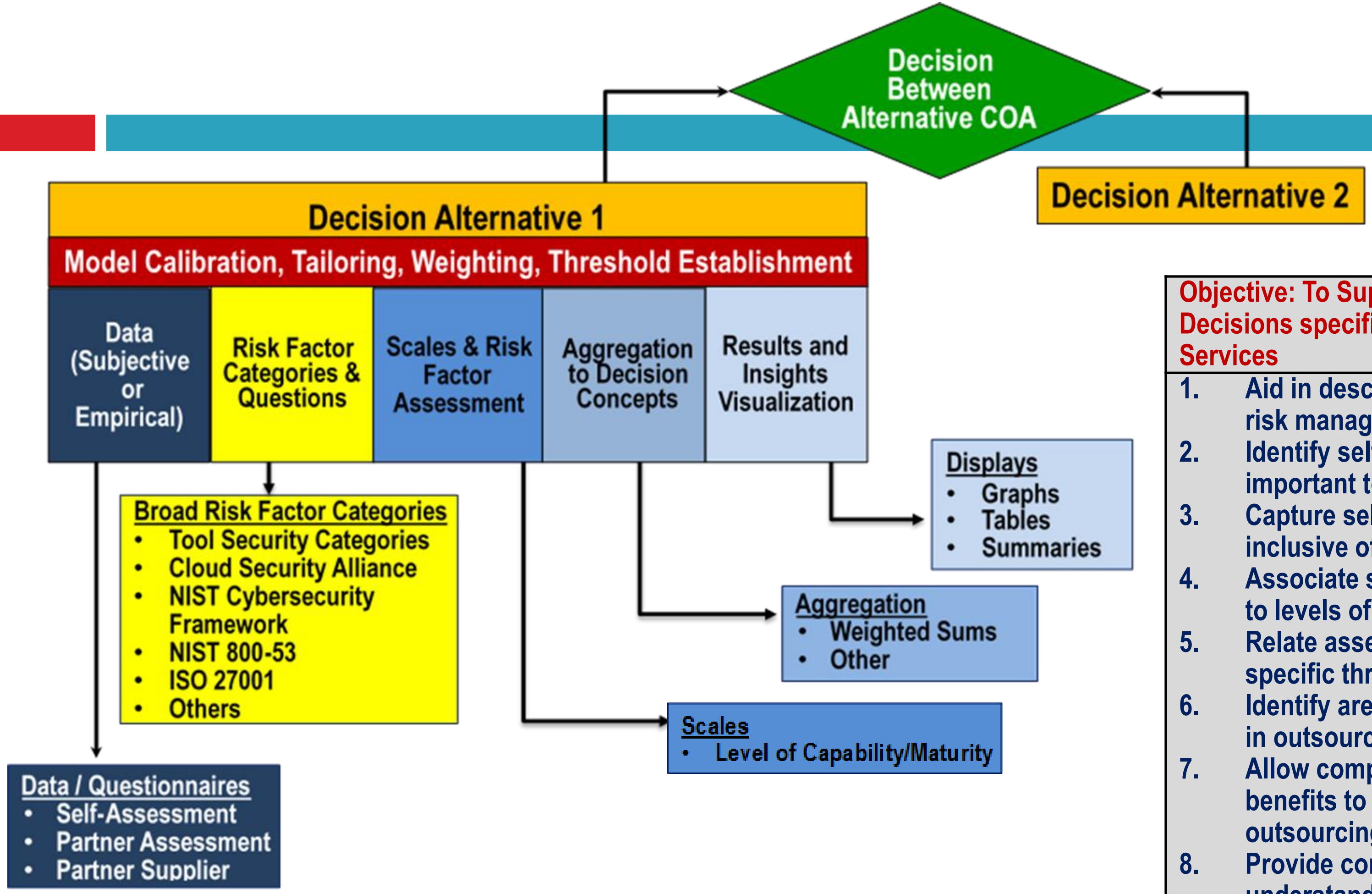
Experts from industry, academia, and government are examining the business and technical risks faced as a result of outsourcing network management services.

- **Whitepaper**
  - Informs the community on risks of outsourced network services
  - Documents the group's findings and recommendations
  - Presents a consistent assessment methodology to address the risk of outsourcing network services
- **Assessment Tool (Prototype)**
  - For use by public and private organizations to determine their total risk picture for outsourcing network services
  - Implements a consistent methodology for examining and mitigating risk, ensures linkage across business and technical aspects, and incorporates recommended best practices
- **Tool Guidance**
  - Accompanies the assessment tool to inform organizations on how to most effectively use the tool including how to weight categories of data and to vet potential courses of action
  - Complements other Supply Chain Risk Management (SCRM) standards and efforts

Goals of the Tool

- To Assist in Discussing and Informing Risk Management Decisions
- Provide a Consistent Framework for Assessing Alternative Courses of Action
- Use available Evidence and Analysis Results to Estimate Level of Maturity of Critical Processes That Help to Mitigate Risk Due to Outsourced Network Services
- Leverages and aligns with existing standards, frameworks, and assessment tools
  - NIST
  - ISO
  - Cloud Security Alliance
  - Others

Tool Prototype Model Framework



Decision Between Alternative COA

Decision Alternative 1

Decision Alternative 2

Model Calibration, Tailoring, Weighting, Threshold Establishment

Data (Subjective or Empirical)

Risk Factor Categories & Questions

Scales & Risk Factor Assessment

Aggregation to Decision Concepts

Results and Insights Visualization

Displays
- Graphs
- Tables
- Summaries

Aggregation
- Weighted Sums
- Other

Broad Risk Factor Categories
- Tool Security Categories
- Cloud Security Alliance
- NIST Cybersecurity Framework
- NIST 800-53
- ISO 27001
- Others

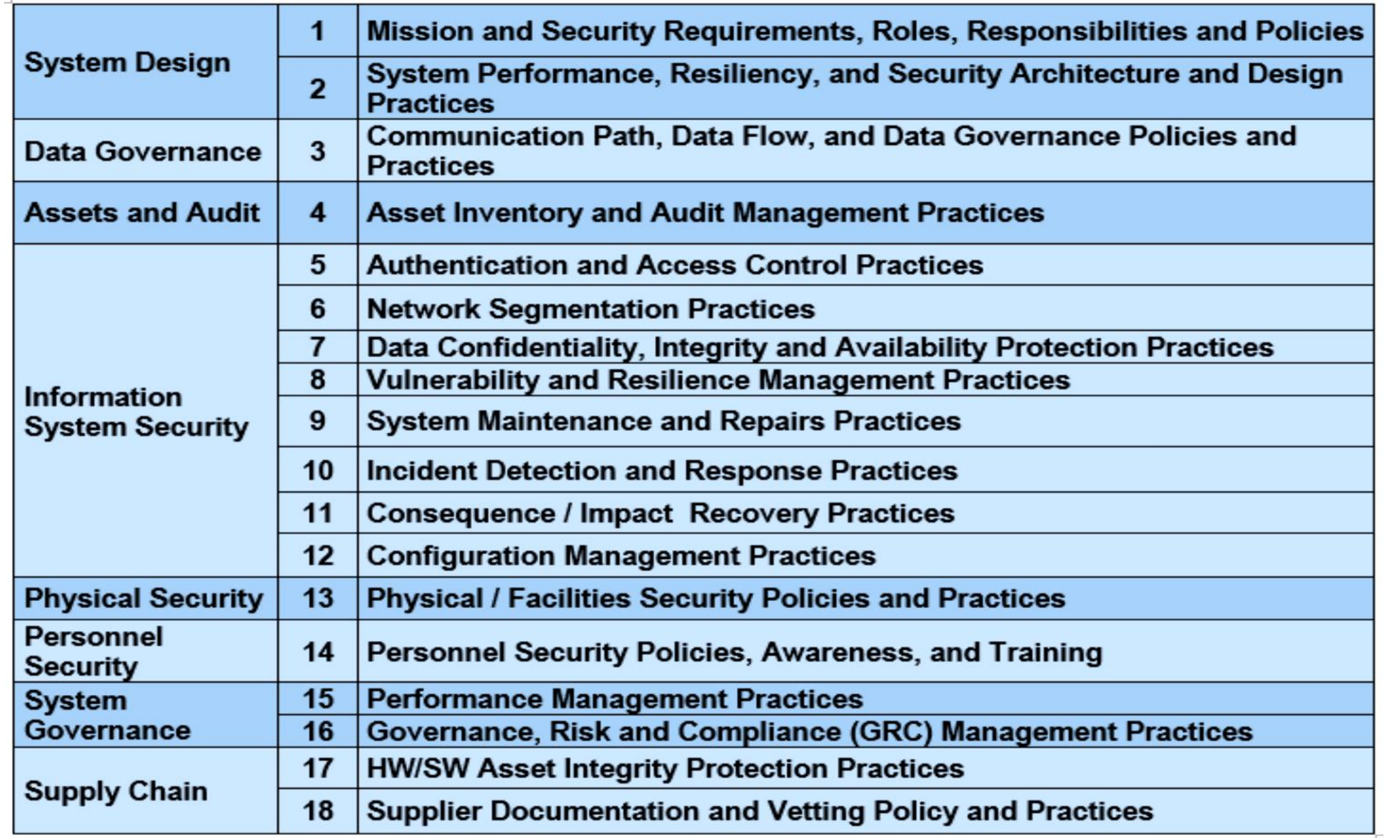
Scales
- Level of Capability/Maturity

Data / Questionnaires
- Self-Assessment
- Partner Assessment
- Partner Supplier

Objective: To Support Risk Management Decisions specific to Outsourcing of Network Services

1. Aid in describing specific outsourcing risk management decisions
2. Identify self and partner characteristics important to managing risks
3. Capture self and partner assessments inclusive of important characteristics
4. Associate self and partner assessments to levels of risk
5. Relate assessments to company/agency specific thresholds or guidance
6. Identify areas of weakness and strength in outsourcing risk management
7. Allow company/agency to explore benefits to investing in more mature outsourcing process
8. Provide consistent framework to enable understanding/discussion of outsourcing risk management decisions

Tool Categories of Security Practices

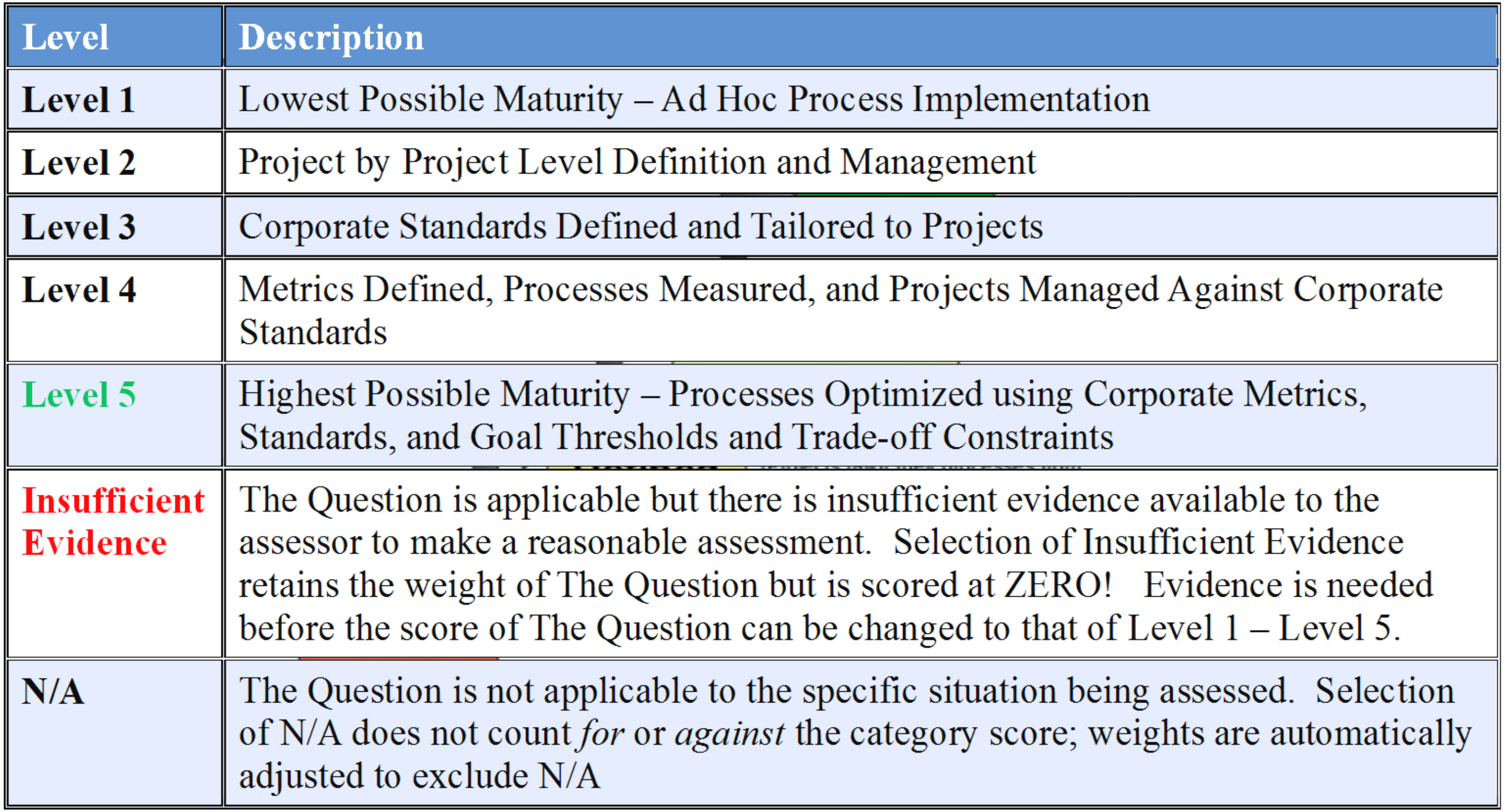


System Design	1	Mission and Security Requirements, Roles, Responsibilities and Policies
	2	System Performance, Resiliency, and Security Architecture and Design Practices
Data Governance	3	Communication Path, Data Flow, and Data Governance Policies and Practices
Assets and Audit	4	Asset Inventory and 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

Industry & Government Standards & Frameworks

- NIST CSF
- NIST 800-30/800-53/800-161
- ISO 27001
- MITRE Resiliency
- CMU/SEI Insider
- Baldridge Cybersecurity
- Cloud Security Alliance

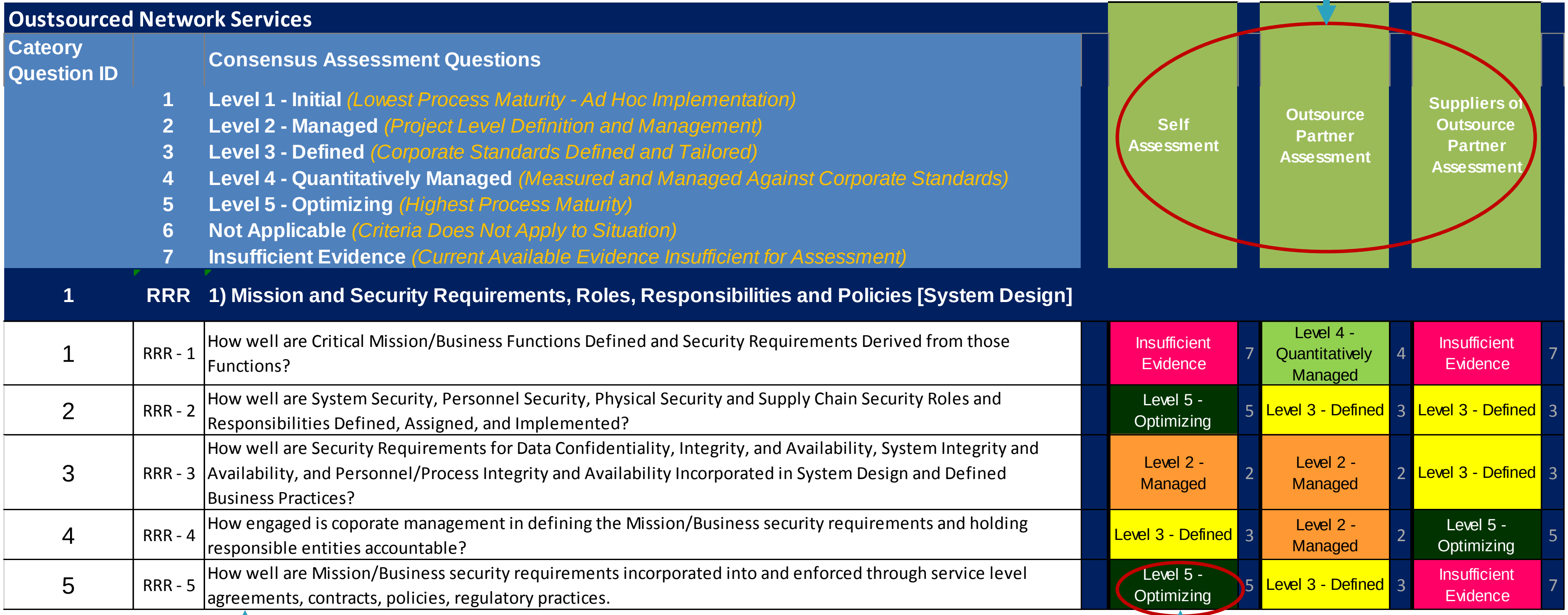
Scale Levels – Focus on Improvement



Level	Description
Level 1	Lowest Possible Maturity – Ad Hoc Process Implementation
Level 2	Project by Project Level Definition and Management
Level 3	Corporate Standards Defined and Tailored to Projects
Level 4	Metrics Defined, Processes Measured, and Projects Managed Against Corporate Standards
Level 5	Highest Possible Maturity – Processes Optimized using Corporate Metrics, Standards, and Goal Thresholds and Trade-off Constraints
Insufficient Evidence	The Question is applicable but there is insufficient evidence available to the assessor to make a reasonable assessment. Selection of Insufficient Evidence retains the weight of The Question but is scored at ZERO! Evidence is needed before the score of The Question can be changed to that of Level 1 – Level 5.
N/A	The Question is not applicable to the specific situation being assessed. Selection of N/A does not count *for* or *against* the category score; weights are automatically adjusted to exclude N/A

Input Assessment Example
Based on Available Evidence

3 Perspectives of Assessment



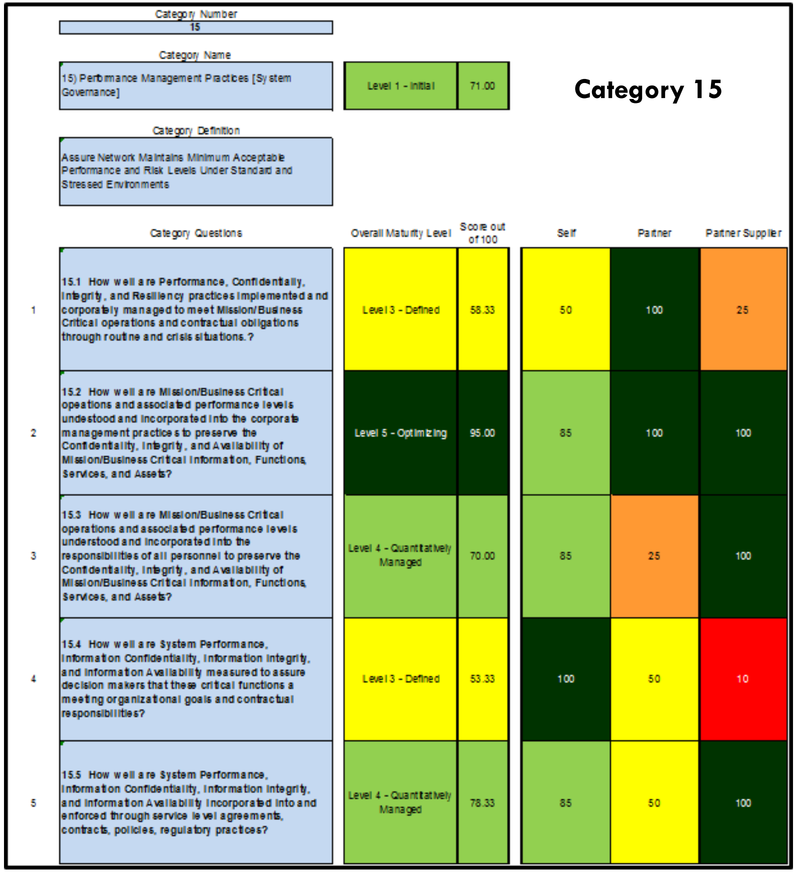
Outsourced Network Services								
Cateory Question ID		Consensus Assessment Questions	Self Assessment		Outsource Partner Assessment		Suppliers of Outsource Partner Assessment	
	1	**Level 1 - Initial** *(Lowest Process Maturity - Ad Hoc Implementation)*						
	2	**Level 2 - Managed** *(Project Level Definition and Management)*						
	3	**Level 3 - Defined** *(Corporate Standards Defined and Tailored)*						
	4	**Level 4 - Quantitatively Managed** *(Measured and Managed Against Corporate Standards)*						
	5	**Level 5 - Optimizing** *(Highest Process Maturity)*						
	6	**Not Applicable** *(Criteria Does Not Apply to Situation)*						
	7	**Insufficient Evidence** *(Current Available Evidence Insufficient for Assessment)*						
1	**RRR**	**1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]**						
1	RRR - 1	How well are Critical Mission/Business Functions Defined and Security Requirements Derived from those Functions?	Insufficient Evidence	7	Level 4 - Quantitatively Managed	4	Insufficient Evidence	7
2	RRR - 2	How well are System Security, Personnel Security, Physical Security and Supply Chain Security Roles and Responsibilities Defined, Assigned, and Implemented?	Level 5 - Optimizing	5	Level 3 - Defined	3	Level 3 - Defined	3
3	RRR - 3	How well are Security Requirements for Data Confidentiality, Integrity, and Availability, System Integrity and Availability, and Personnel/Process Integrity and Availability Incorporated in System Design and Defined Business Practices?	Level 2 - Managed	2	Level 2 - Managed	2	Level 3 - Defined	3
4	RRR - 4	How engaged is coporate management in defining the Mission/Business security requirements and holding responsible entities accountable?	Level 3 - Defined	3	Level 2 - Managed	2	Level 5 - Optimizing	5
5	RRR - 5	How well are Mission/Business security requirements incorporated into and enforced through service level agreements, contracts, policies, regulatory practices.	Level 5 - Optimizing	5	Level 3 - Defined	3	Insufficient Evidence	7

5 Questions Per Category

(Questions Span Category Concepts and Controls)

Process Maturity/Capability Level Assessment

Evaluation of a Security Practice



Category 15

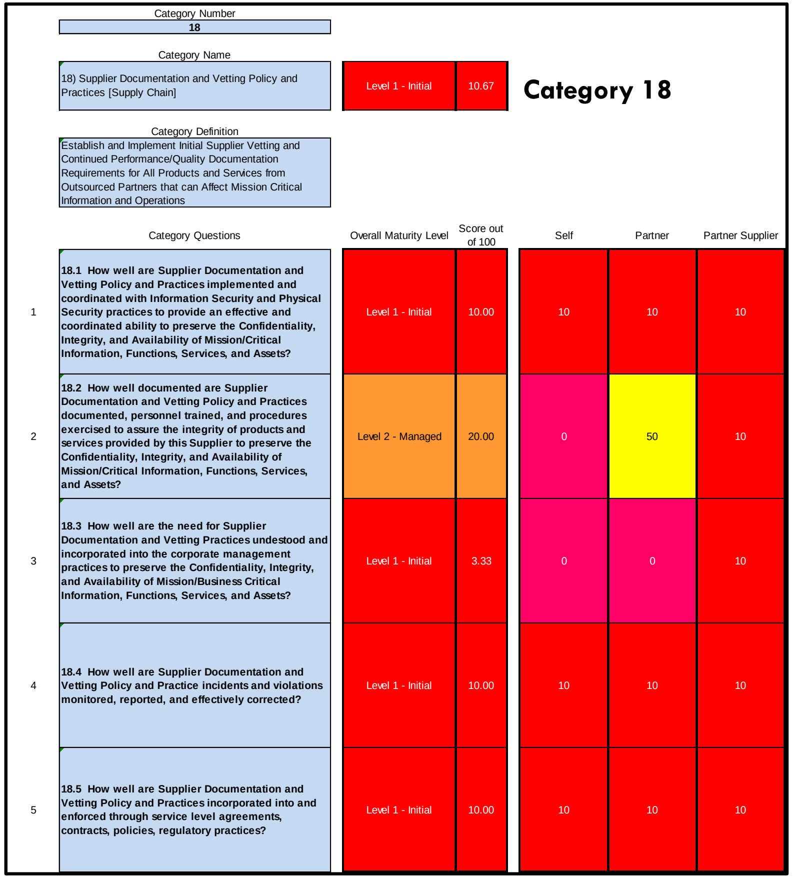
Category Number
15

Category Name
15) Performance Management Practices [System Governance]

Level 1 - Initial | 71.00

Category Definition
Assure Network Maintains Minimum Acceptable Performance and Risk Levels Under Standard and Stressed Environments

	Category Questions	Overall Maturity Level	Score out of 100	Self	Partner	Partner Supplier
1	15.1 How well are Performance, Confidentially, Integrity, and Resiliency practices implemented and corporately managed to meet Mission/Business Critical operations and contractual obligations through routine and crisis situations.?	Level 3 - Defined	58.33	50	100	25
2	15.2 How well are Mission/Business Critical opeations and associated performance levels undestood and incorporated into the corporate management practices to preserve the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets?	Level 5 - Optimizing	95.00	85	100	100
3	15.3 How well are Mission/Business Critical operations and associated performance levels understood and incorporated into the responsibilities of all personnel to preserve the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets?	Level 4 - Quantitatively Managed	70.00	85	25	100
4	15.4 How well 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?	Level 3 - Defined	53.33	100	50	10
5	15.5 How well are System Performance, Information Confidentiality, Information Integrity, and Information Availability incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?	Level 4 - Quantitatively Managed	78.33	85	50	100



Category 18

Category Number
18

Category Name
18) Supplier Documentation and Vetting Policy and Practices [Supply Chain]

Level 1 - Initial | 10.67

Category Definition
Establish and Implement Initial Supplier Vetting and Continued Performance/Quality Documentation Requirements for All Products and Services from Outsourced Partners that can Affect Mission Critical Information and Operations

	Category Questions	Overall Maturity Level	Score out of 100	Self	Partner	Partner Supplier
1	18.1 How well 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?	Level 1 - Initial	10.00	10	10	10
2	18.2 How well documented 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?	Level 2 - Managed	20.00	0	50	10
3	18.3 How well are the need for Supplier Documentation and Vetting Practices undestood and incorporated into the corporate management practices to preserve the Confidentiality, Integrity, and Availability of Mission/Business Critical Information, Functions, Services, and Assets?	Level 1 - Initial	3.33	0	0	10
4	18.4 How well are Supplier Documentation and Vetting Policy and Practice incidents and violations monitored, reported, and effectively corrected?	Level 1 - Initial	10.00	10	10	10
5	18.5 How well are Supplier Documentation and Vetting Policy and Practices incorporated into and enforced through service level agreements, contracts, policies, regulatory practices?	Level 1 - Initial	10.00	10	10	10

Summary View By Security Practice

	Maturity of RMONS Solutions	Overall Maturity Level	Score	Self	Partner	Source
1	**1) Mission and Security Requirements, Roles, Responsibilities and Policies [System Design]**	Level 3 - Defined	47.33	55.00	47.00	40.00
2	**2) System Performance, Resiliency, and Security Architecture and Design Practices [System Design]**	Level 3 - Defined	38.33	29.00	34.00	52.00
3	**3) Communication Path, Data Flow, and Data Governance Policies and Practices [Data**	Level 3 - Defined	50.42	46.25	46.25	58.75
4	**4) Asset Inventory and Audit Management Practices [Asset and Audit]**	Level 3 - Defined	47.78	45.00	78.33	20.00
5	**5) Authentication and Access Control Practices [Info. Sys.Security]**	Level 3 - Defined	58.33	81.00	52.00	42.00
6	**6) Network Segmentation Practices [Info. Sys.Security]**	Level 3 - Defined	40.00	39.00	35.00	46.00
7	**7) Data Confidentiality, Integrity and Availability Protection Practices [Info. Sys.Security]**	Level 3 - Defined	65.56	61.67	65.00	70.00
8	**8) Vulnerability and Resilience Management Practices [Info. Sys.Security]**	Level 3 - Defined	53.33	70.00	25.00	65.00
9	**9) Configuration Management Practices [Info. Sys.Security]**	Level 2 - Managed	35.00	18.75	42.50	43.75
10	**10) System Maintenance and Repairs Practices [Info. Sys.Security]**	Level 3 - Defined	63.89	65.00	56.67	70.00
11	**11) Incident Detection and Response [Info. Sys.Security]**	Level 3 - Defined	53.33	48.75	52.50	58.75
12	**12) Consequence / Impact Recovery Policies and Practices [Info. Sys.Security]**	Level 3 - Defined	45.00	45.00	45.00	45.00
13	**13) Physical / Facilities Security Policies and Practices [Physical Security]**	Level 2 - Managed	37.33	31.00	44.00	37.00
14	**14) Personnal Security Policies, Awareness, and Training [Personnel Security]**	Level 3 - Defined	54.17	61.25	51.25	50.00
15	**15) Performance Management Practices [System Governance]**	Level 4 - Quantitatively Managed	71.00	81.00	65.00	67.00
16	**16) Governance, Risk, and Compliance (GRC) Management Practices [System Governance]**	Level 3 - Defined	50.67	52.50	52.50	47.00
17	**17) Asset HW/SW Integrity Protection Practices [Supply Chain]**	Level 3 - Defined	55.42	42.50	62.50	61.25
18	**18) Supplier Documentation and Vetting Policy and Practices [Supply Chain]**	Level 1 - Initial	10.67	6.00	16.00	10.00

Aggregated Conceptual Views for Management

	Overall Maturity Level	Score	Self	Partner	Source
Overall	Level 3 - Defined	48.75	48.81	48.36	49.08

Maturity Addressing RMONS Problems	Overall Maturity Level	Score
Providing Insider Level Access and Privilege	Level 3 - Defined	49.60
Providing Mission Critical Information and Assets	Level 3 - Defined	51.17
Accepting Mission Critical Products and Services	Level 2 - Managed	33.04
Allowing Thrid Party to Provide Representation	Level 2 - Managed	32.42

Maturity of RMONS Solutions	Overall Maturity Level	Score	Self	Partner	Source
System Design Practices	Level 3 - Defined	42.83	42.00	40.50	46.00
Data Governance Practices	Level 3 - Defined	50.42	46.25	46.25	58.75
Asset and Audit Practices	Level 3 - Defined	47.78	45.00	78.33	20.00
INFOSEC Practices	Level 3 - Defined	51.81	53.65	46.71	55.06
PHYSEC Practices	Level 2 - Managed	37.33	31.00	44.00	37.00
PERSEC Practices	Level 3 - Defined	54.17	61.25	51.25	50.00
System Governance Practices	Level 3 - Defined	60.83	66.75	58.75	57.00
Supply Chain Security Practices	Level 2 - Managed	33.04	24.25	39.25	35.63

Where are we?

- Initial Problem Exploration
- Developing a Conceptual Framework for Solutions
- Researching Related Concepts
- Mapping Existing Frameworks to Problems Space
- Filling Gaps, Refining Concepts
- Drafting a White Paper and Building a Prototype Tool
- Publishing White Paper and Making Prototype Tool Available