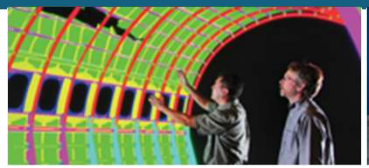
OFFICIAL USE ONLY

Sandia National Laboratories

Secure Supply Chain

Mitigating Risk in the Software Acquisition Process




PRESENTED BY

Emily Lies

Supply Chain Risk Management

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Content Notes

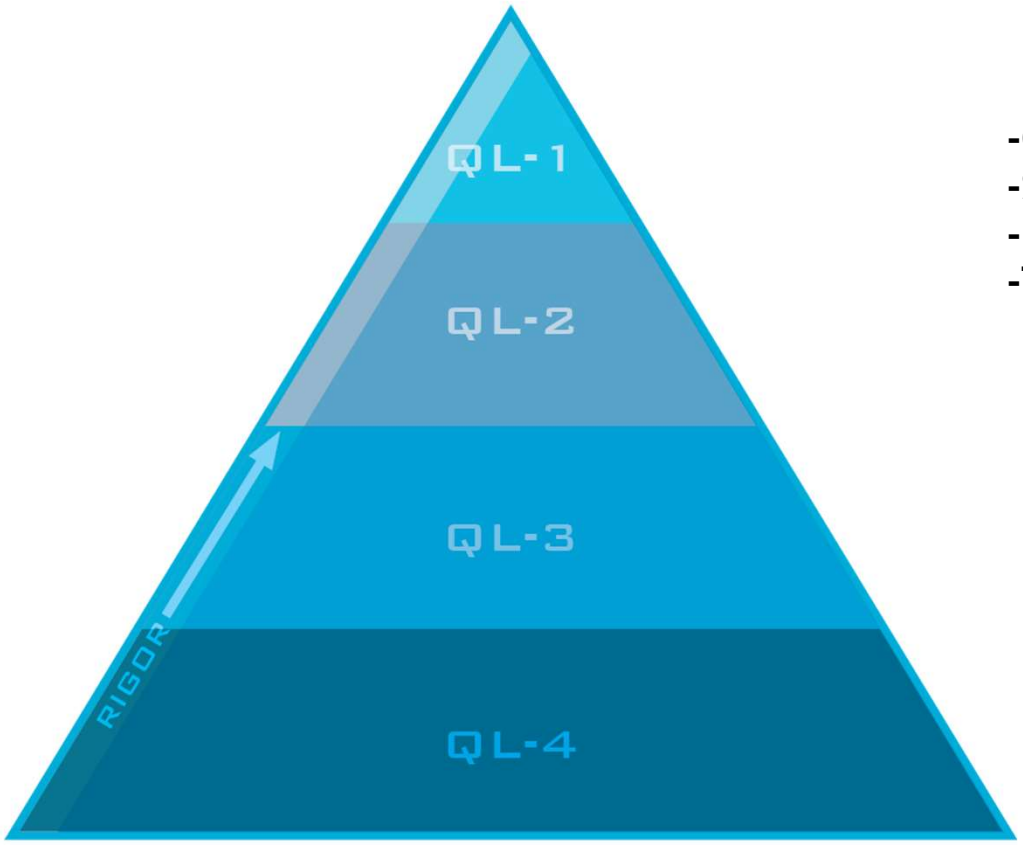
Information Sensitivity

The combined process and tools that NTESS uses to conduct Subcontractor Risk Assessments (discussed herein) is Official Use Only/Controlled Unclassified Information. The methodology is Nuclear Deterrence Mission Sensitive and should be controlled to prevent public release, as release of the information may be harmful to DOE/NNSA mission areas. Please do not share it outside of your organization without consent. Do not share with vendors or other third-parties.

Comment concerning references to external/commercial data sources

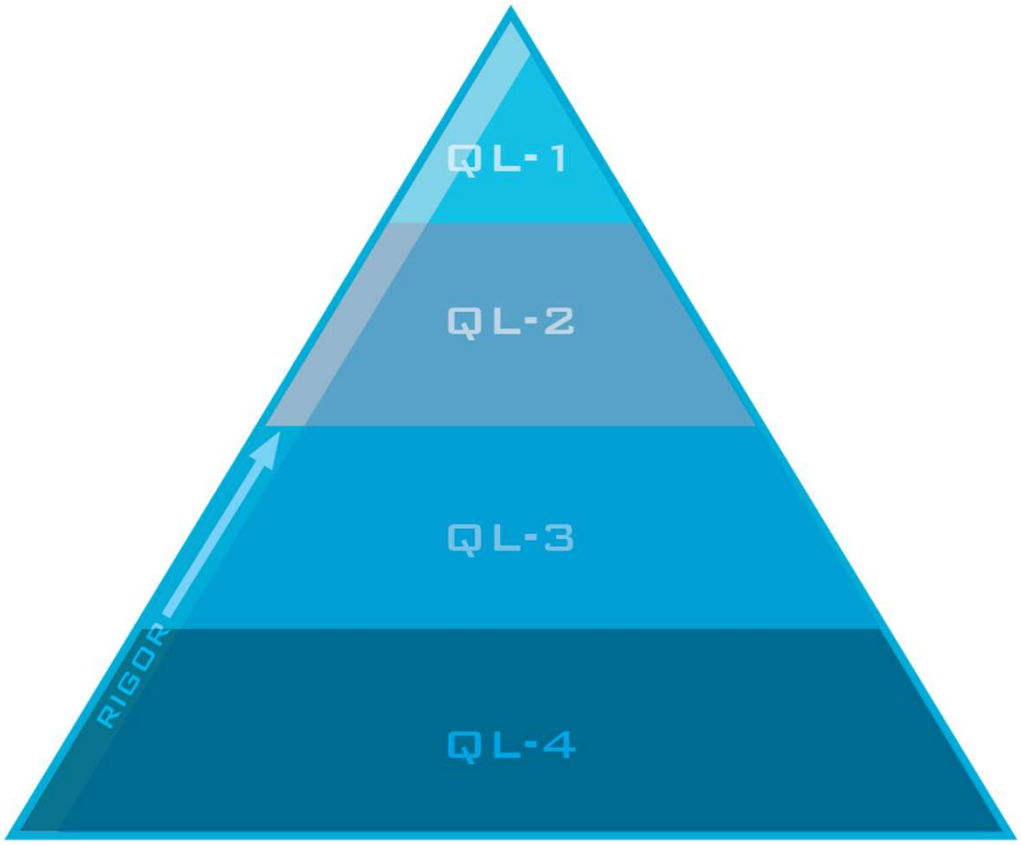
This presentation references external data sources requiring a paid subscription. NTESS does not specifically endorse these data source providers. Multiple data source options are available. The examples are provided to enhance understanding of NTESS's current Subcontractor Risk Assessment process.

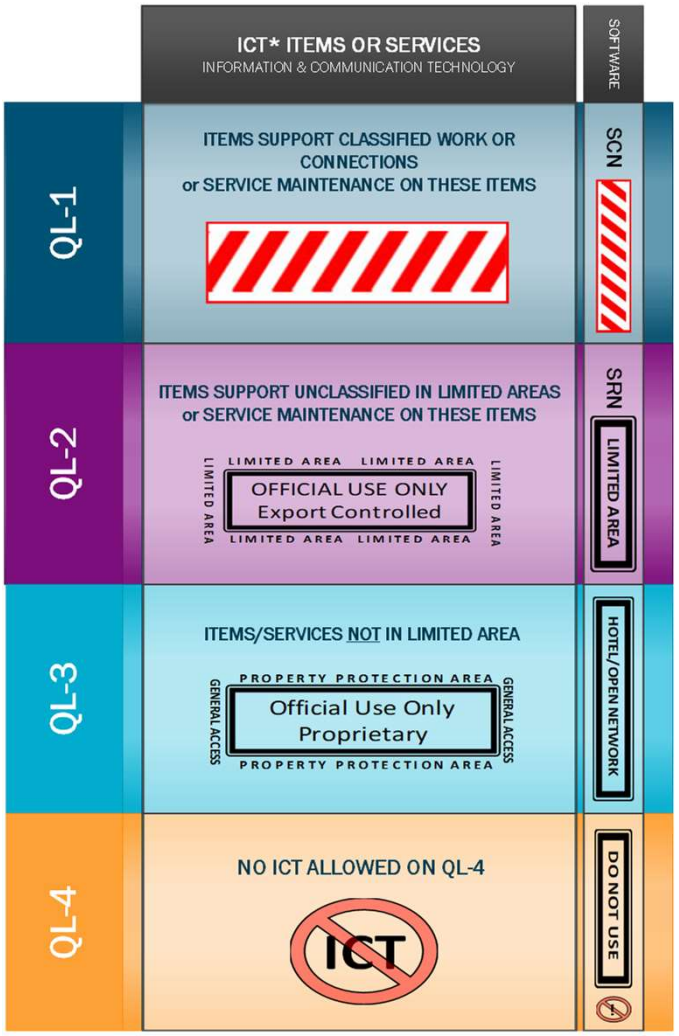
SNL's Graded Approach



-Choose level of rigor for software
-Supplier Assessments
-Inspection Requirement
-Terms & Conditions to mitigate software risk

Level of Rigor

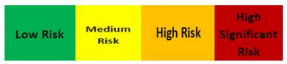


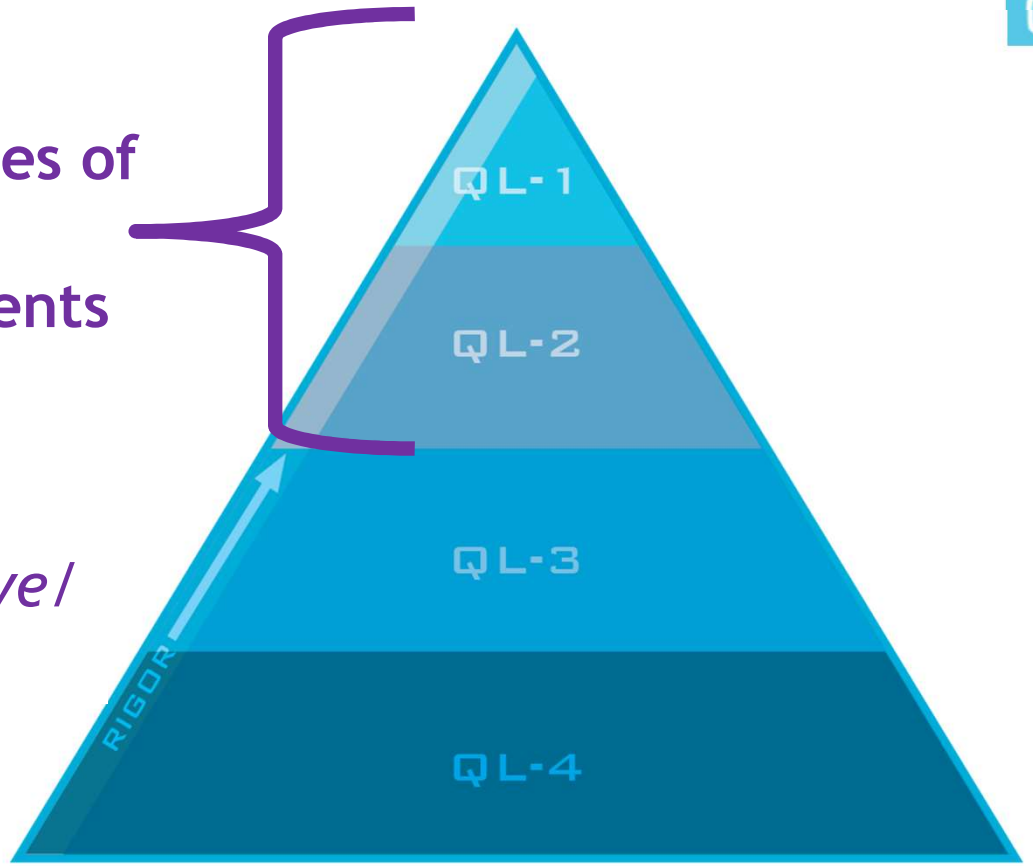


*Information and Communication Technology (ICT): Any device, application, or service that enables users to access, store, transmit, share, or manipulate information or data. This includes, but is not limited to, computers, telephones, software, equipment that uses software, middleware, storage systems, audio visual systems, and satellite systems and services supporting their use or operation.

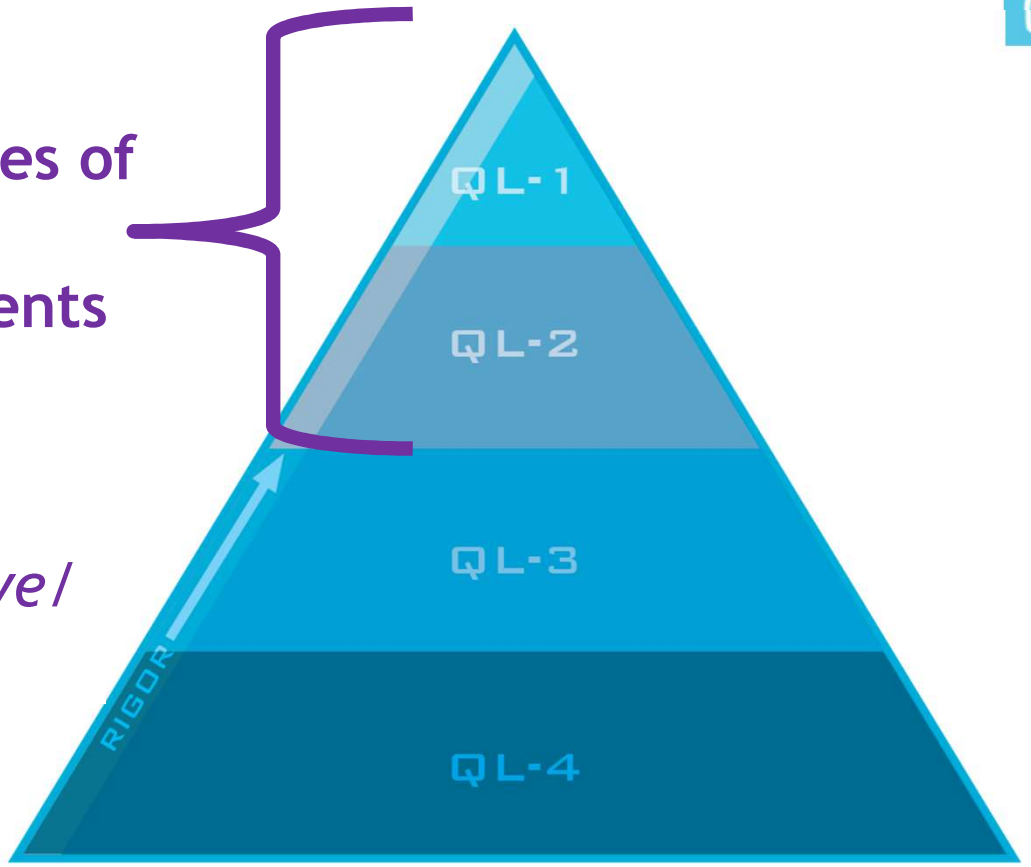
TWO types of Supplier Assessments

- ✓ *Internal Only*
- ✓ *Interactive/ Shared*





TWO types of Supplier Assessments



- ✓ *Internal Only*

- ✓ *Interactive/ Shared*

QL-2: Desk Assessment

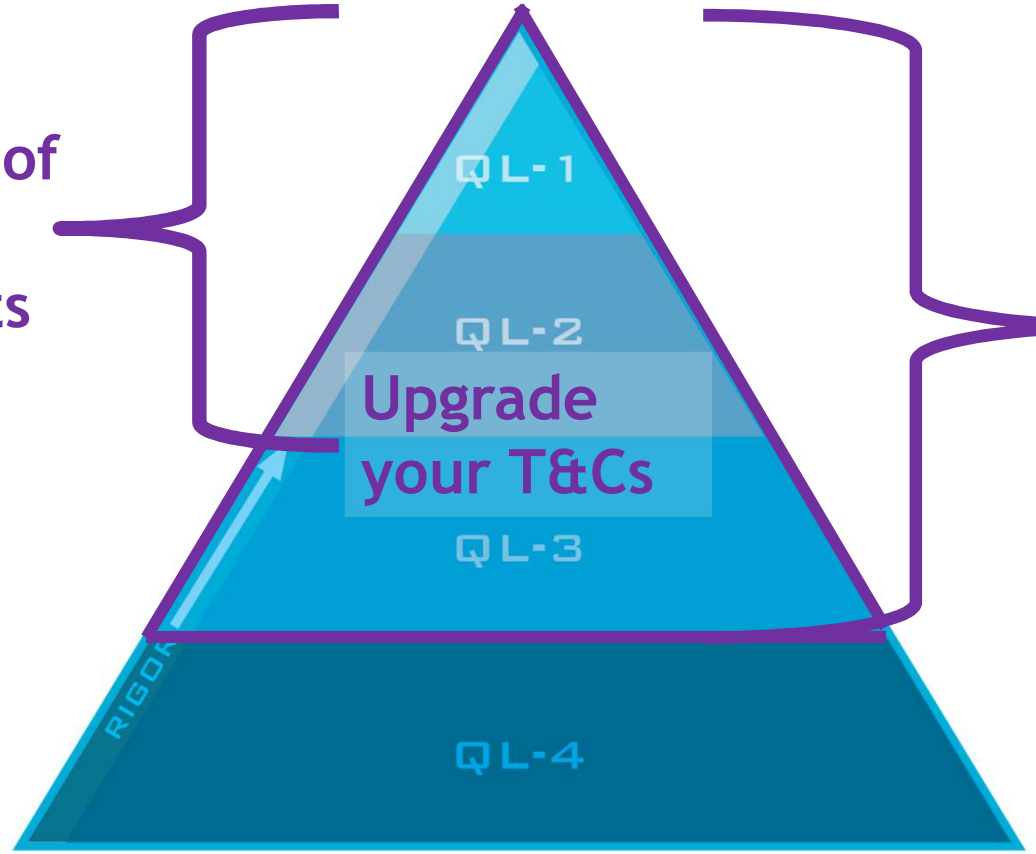
7

Yes	No	N/A	
☐	☐	☐	1. Does your organization have a documented process for gathering system/program/product requirements and/or customer requirements? (a) If Yes, please describe: (b) If No, please explain:
☐	☐	☐	2. Does your organization employ static testing methods on all products/deliverables? *Distributors: Can you supply documentation from the manufacturer demonstrating static testing was performed on deliverables?* COMMENTS:
☐	☐	☐	3. Does your organization employ dynamic testing methods on all products/deliverables? (a) If Yes, please describe: (b) If No, please explain: *Distributors: Can you supply documentation from the manufacturer supporting the use of dynamic testing methods? (Y/N)* *(a) If Yes, please attach.* *(b) If No, please explain:*

Desk Assessment

SCAN Database

TWO types of Supplier Assessments



Documented Inspection of Deliverable

SOFTWARE, SERVICES & INFORMATION SYSTEMS SECURITY ASSURANCE

1. Subcontractor warrants that all items, information systems, software and services, including cloud-based service models (e.g., infrastructure as a service, platform as a service, or software as a service) delivered under this Subcontract only contain features and/or functions that are fully disclosed.
2. If Subcontractor suspects or becomes aware of any threat events, security incidents, or vulnerabilities that may have the potential to affect the functionality, security, or integrity of items or services provided to NTESS, Subcontractor shall immediately give verbal notice to NTESS' Security Incident Management Program (SIMP) by calling (505) 283-7467, or for subcontracts issued in California call 1-(925)294-2600 (these phone lines are manned 24 hours a day, 7 days a week). Verbal notification shall occur at the time of Subcontractor's awareness or suspicion, and prior to any follow up investigations. In addition to the immediate verbal notification, Subcontractor shall provide written notification to the SP and SDR (if an SDR is named in the Subcontract) within 72 hours of Subcontractor's awareness or suspicion.
3. Subcontractor shall cooperate fully with NTESS to investigate all potential security incidents, threat events, and/or vulnerabilities.

NOTE: As used in this clause, the terms "threat event" and "vulnerability" have the meanings defined in NIST SP 800-30. The term "security incident" has the meaning defined in NIST SP 800-53. Security incidents include, but are not limited to: malfunctions due to design/implementation errors and omissions, targeted malicious attacks, untargeted malicious attacks, insider threats, unintended capabilities, and compromises/breaches involving information system components, information technology products, and development processes or personnel.

DISCLOSING USE OF FREE, LIBRE AND OPEN SOURCE SOFTWARE (FLOSS)

Subcontractor shall disclose in writing, and obtain NTESS written consent, before using any FLOSS licenses or delivering any FLOSS in connection with this subcontract. Send written disclosures to the SP listed on this first page of this subcontract. NTESS may withhold written consent for use or delivery of FLOSS at its sole discretion.

FLOSS refers to software that incorporates, embeds, uses, bundles, or otherwise associates with any of the following:

1. Open source, publicly available, or "free" software, library or documentation;

2. Software licensed under a FLOSS License;

3. Software provided under a license that (a) subjects the delivered software to any FLOSS License, or (b) requires the delivered software to be licensed for the purpose of making derivative works or be redistributable at no charge.

FLOSS License(s) include any Free Software, Open Source and Public License(s). FLOSS License also refers to: the General Public License (GPL), Lesser/Library GPL (LGPL), the Affero GPL (APL), the Apache license, the Berkeley Software Distribution ("BSD") license, the MIT license, the Artistic License (e.g., PERL), the Mozilla Public License (MPL), or variations thereof.

Software Development

NTESS maintains an objective for Subcontractor development of secure, reliable, resilient, and assured software. The security controls cited in this clause can be traced back to National Institute of Science and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

- Subcontractor shall create and deliver a secure coding guide according to the schedule outlined in the Statement of Work. At a minimum, the coding guide shall specify:

  a. A configuration management plan, with provisions for backup and disaster recovery;

  b. The coding language choice;

  c. Coding standards;

  d. Inspection and test strategy;

  e. Peer review strategy; and

  f. Software release strategy

- Subcontractor shall implement and document peer reviews during development. At least one (1) review shall include the SDR or SDR's delegate. For Subcontracts with multi-year performance periods, Subcontractor shall provide the SDR written notice of scheduled reviews at least five (5) business days in advance, and shall permit NTESS participation in at least 1 peer review per year. Notes documenting other peer reviews shall be provided to the SDR upon request.

- Subcontractor shall review development processes and product against the Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), and the Open Web Application Security Project (OWASP). Subcontractor shall document and date CWE, CVE, and OWASP reviews and provide these to the SDR upon request.

- Subcontractor shall perform an origin analysis of all third-party libraries and frameworks used and ensure the versions used in the delivered software have no known vulnerabilities reported in industry databases such as those listed in section 3 of this clause.

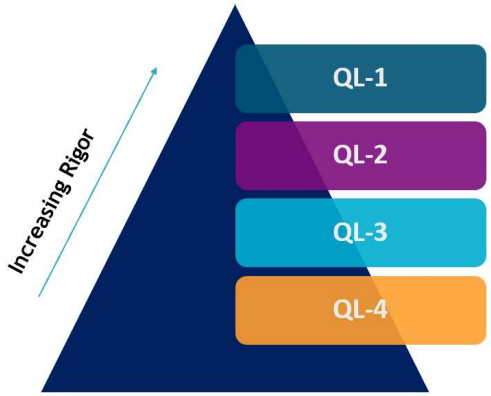
QUESTIONS??

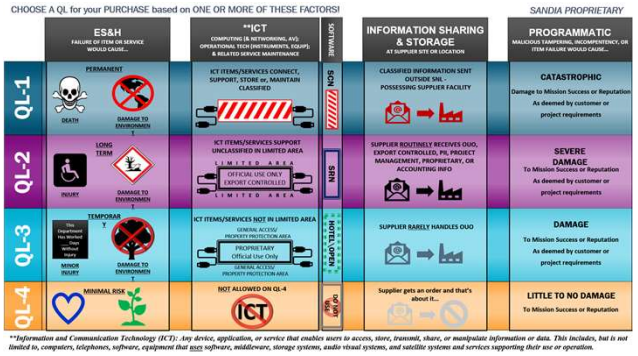
Backup Slides

SCRM Programs to Infuse TRUST into NTESS's Supply Chain

PURCHASE REQUISITION	RFQ/AWARD	POST-AWARD

Quality Level Program





Independent Analytics On Suppliers:
SCRM-A Dashboard & Subcontractor Risk Assessments

Risk Category	
OVERALL RISK RATING	High
RESTRICTED PARTY SCREENING	Low
FINANCIAL HEALTH	Low
RISK EVENTS	High-Sig
COUNTERFEIT INDICATORS	Low
PAST PERFORMANCE WITH SANDIA	Low
FOREIGN CORPORATE LINKAGES	High
NON-US LABOR	Low
LOWER TIER SUPPLY CHAIN	High

Engaging Suppliers: At-Site & Desk Assessments

SCAN/AEA

Quality Level	Source	Assessment Date	Expiration Date
N/A	AEA	7/2/2019	7/1/2020
QL-1	SCAN	9/1/2018	9/17/2021
QL-2	SCAN	1/7/2019	1/6/2022

Assess

NextGen SCORE Performance

All Subcontracts:

On-Time	Quality	Satisfied
Yes	Yes	Yes

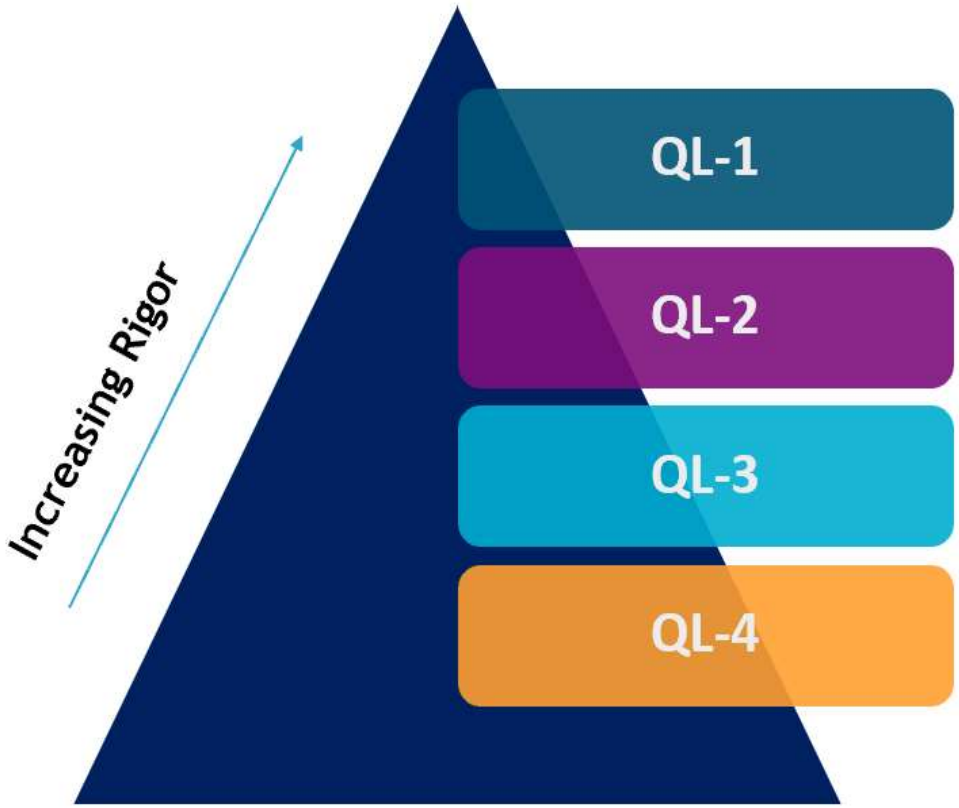
Construction Subcontracts:

On-Time	Quality	Satisfied	Project Mgmt	Safety
Yes	Yes	Yes	Yes	Yes

Inspect & Report

Suspect / Counterfeit Items

Purchase Requisition: the Graded Approach



+++Increased Rigor Interactive Assessment (At-Site)

++Two Types of Subcontractor Assessments (internal/interactive)

+Documented Inspection of Deliverable

No Additional Requirements