North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Industry Coordinated Supply Chain Activities

North American Transmission FORUM

Introduction

Tom Galloway, President and CEO, NATF

Agenda for Today's Webinar

Overview

Alignment of industry/other organizations

- Trades, Forums and participating organizations
- Suppliers
- Assessors

Web Page Overview

The NATF Criteria

The Model for Supplier Evaluations (Model)

Implementation: resources and tools

Next Steps

Objectives for Today's Webinar

Provide an overview of the Supplier Cyber Security Assessment Model

- Convergence on use of the Model
- How the Model Works
- Contributing Organizations
- Where to find information

Identify whether there is a need for future industry webinars or workshops

Look ahead at upcoming projects

Overview - Objectives of Supply Chain Activities

Industry Convergence

- Achieve industry convergence on the approach (Model) to facilitate addressing the following objectives

Security

- Identifying and addressing cyber security risks introduced via supply chain

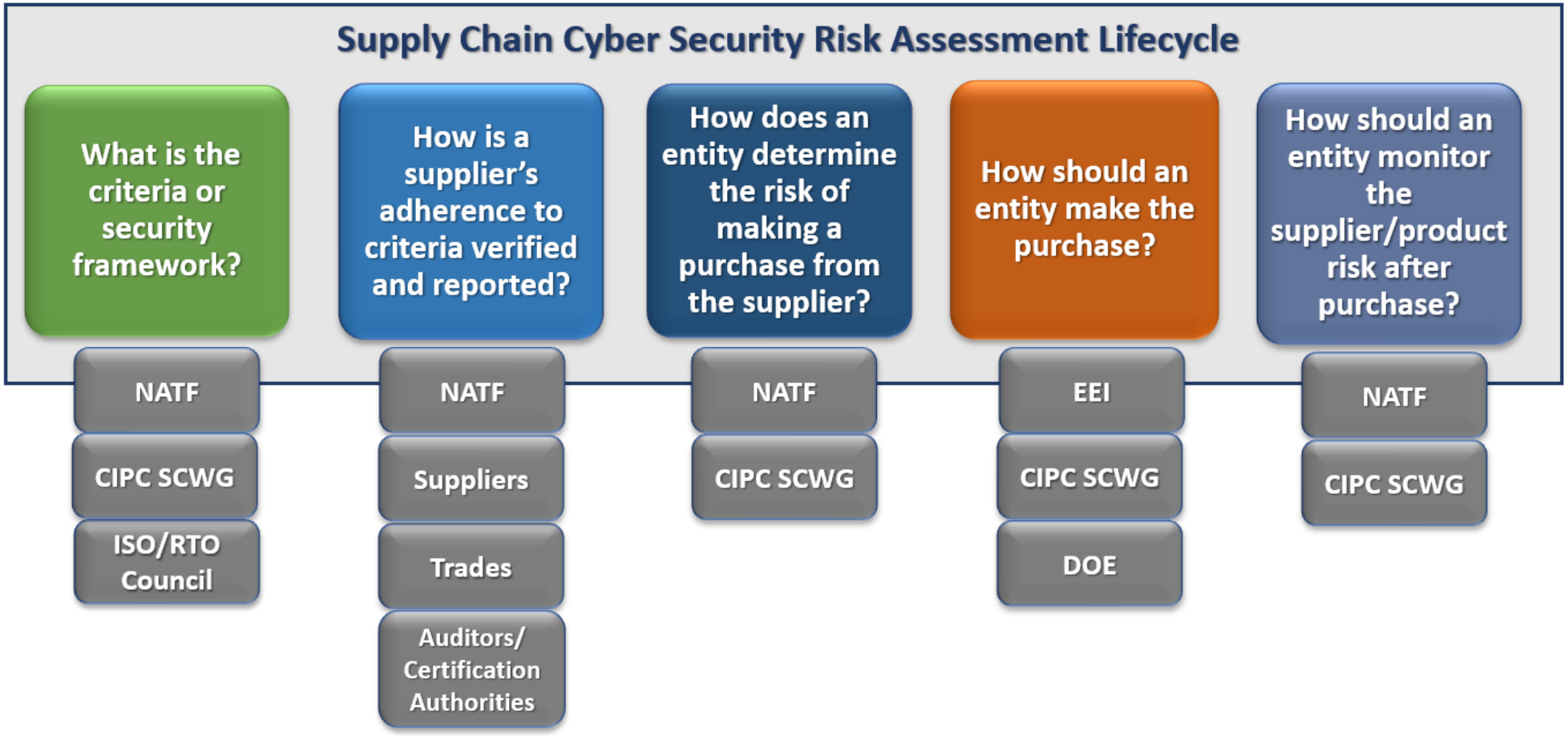
Efficiency and Effectiveness

- Convergence on common approaches to achieve reasonable assurance of suppliers' security practices

Compliance

- Implementation guidance to meet supply chain related CIP standards (CIP-013-1; CIP-005-6 R2.4; CIP-010-3 R1.6)

Overview – Build on existing Supply Chain Work



Overview - Supply Chain Activities to Date

NATF Supply Chain Criteria Team

NATF Supply Chain Steering Team

NATF Proof of Concept Team

NATF-led Industry Organizations Team

- June 2019 — NATF Criteria Version 0
- July 2019 — NATF Criteria Application Guide
- October 2019 — NATF Proof of Concept Team Strawman
- December 2019 — Industry Organizations' Team alignment on Supplier Assessment Model
- January 30 — NATF Criteria Refinement, EEI Procurement Language Refinement
- In Progress — Questionnaire, Additional Projects

North American Transmission FORUM

Alignment of Organizations

A list of participating organizations is available on the NATF Public Website:

https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

Value Proposition

- Broader than Industry Organizations
- *The Supplier Cyber Security Assessment Model and complementary products provide a streamlined, effective, and efficient industry-accepted approach for entities to assess supplier cyber security practices, which, if applied widely, will*
  - *reduce the burden on suppliers,*
  - *provide entities with more and better information and*
  - *improve cyber security.*

Industry Organization Team Members

How is a supplier's adherence to criteria verified and reported?

Proof of Concept October 2019

Organizations, Forums and Working Groups

- EEI
- LPPC
- APPA
- TAPS
- NAGF
- NAESB
- ConEd Working Group
- SCWG/CIPC
- NRECA

Suppliers

- ABB
- GE Grid Software Solutions
- OSI
- Siemens Industry, Inc.
- Schneider Electric
- Schweitzer Engineering

Third-Party Assessors

- Ernst & Young
- KPMG LLP
- PWC
- Deloitte

Vendor Organizations for support products or services

- EPRI
- Fortress/A2V

Industry Organizations' Perspectives

Edison Electric Institute (EEI)

- Kegan Gerard, Manager, Cyber and Infrastructure Security

New York Power Authority

- Representing LPPC, APPA
- Randy Crissman, Sr. Reliability and Resilience Specialist

Supplier Perspective

Open Systems International, Inc. (OSI)

- Rob Koziy, Director of Compliance and Cyber Security

ABB

- Joe Doetzl, Chief Information Security Officer, Power Grids Business

Siemens Industry, Inc.

- Andy Turke, Product & Solution Security Officer

Schweitzer Engineering Laboratories, Inc. (SEL)

- Frank Harrill, Director of Security

Assessors' Perspective

Ernst & Young

- Josh Sandler, Senior Manager
- Jeff Rozek, Managing Director

PricewaterhouseCoopers (PwC)

- Jake Stricker, Managing Director

Deloitte

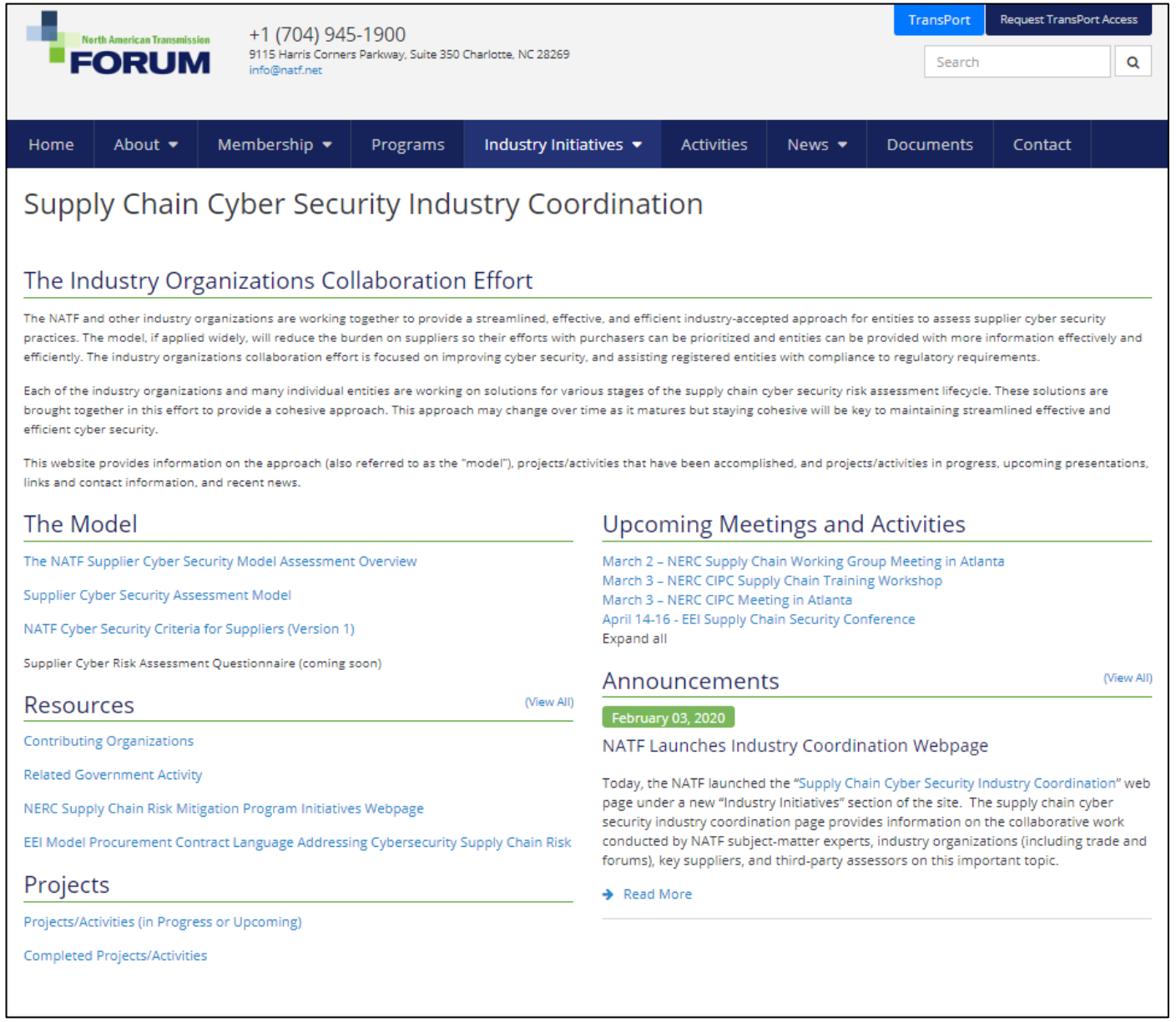
- Matthew Barbera, Senior Manager

The Industry Coordination Web Page

Available on the NATF Public Website:

https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

NATF-hosted web page for Industry Coordination



North American Transmission FORUM

The NATF Criteria

Available on the NATF Public Website:

https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

Establishing Criteria for Evaluations: The NATF Criteria

What is the criteria or security framework?

The NATF Criteria

July 2019

- Version 1 posted on the NATF Public Website
- 60 criteria for supplier supply chain cyber security practices
- 26 organizational information considerations
- Maps to existing frameworks

NATF Criteria Spreadsheet

Open Distribution

			Required by NERC Reliability Standards?		Mapping to Existing Frameworks									
					NIST							CIS Controls v7.1	IEC 62443	ISO 27001
Criteria Identification Number	Risk Area	NATF Cyber Security Supply Chain Criteria for Suppliers Version 1 *(NATF Board Approved)*	Good security practices; exceeds NERC CIP Standards' requirements	CIP-013 requirement or supports other standards	Governance and all criteria NIST SP 800-161, 800-53	Access NIST SP 1800-2	Asset Chg Config - NIST SP 1800-5	Info Protection - NIST SP 800-171	Incident Response - NIST SP 800-184, 800-150, 800-61	Vulnerability Mgmt - NIST SP 800-64, 800-160, 800-82, 800-115, 800-125	Cybersecurity Framework Version 1.1			List other versions 27001.xxxx, 2700 applicable
1	Access Control and Mgmt	Supplier establishes and maintains an identity and access management program that ensures sustainable, secure product manufacturing/development		R1.2.3 R1.2.6	PR.AC 1-5 Rev. 4 AC-1-6 IA Family AC-16-20 CM-7 PE-2-6 PE-9 SC-7						PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-3	CSC 14: Controlled Access Based on the Need to Know CSC 16: Account Monitoring and Control	2.4 SP.03.01 2.4 SP.03.07 2.4 SP.03.08	A.9.1.1 A.9.4.1
2	Access Control and Mgmt	Supplier establishes and maintains a program that ensures storage security at supplier's site (e.g. chain of custody)	x		PR.AC-4 Rev. 4 AC-16 MP-4						PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-3	CSC 14: Controlled Access Based on the Need to Know CSC 16: Account Monitoring and Control	2.4 SP.03.10	A.15.1.2
		Supplier's personnel vetting process allows supplier to share background check		Supports										

North American Transmission FORUM

The Supplier Cyber Security Assessment Model

For further explanation, see the
"Supplier Cyber Security Assessment Model" Document
available on the Supply Chain Industry Coordination page of the NATF Public Website

Supplier Cyber Security Assessment: Steps

Supplier Evaluation

How is a supplier's adherence to criteria verified and reported?

- Obtain information
- Evaluate Information
- Conduct Risk Assessment
- Make Purchase Decision

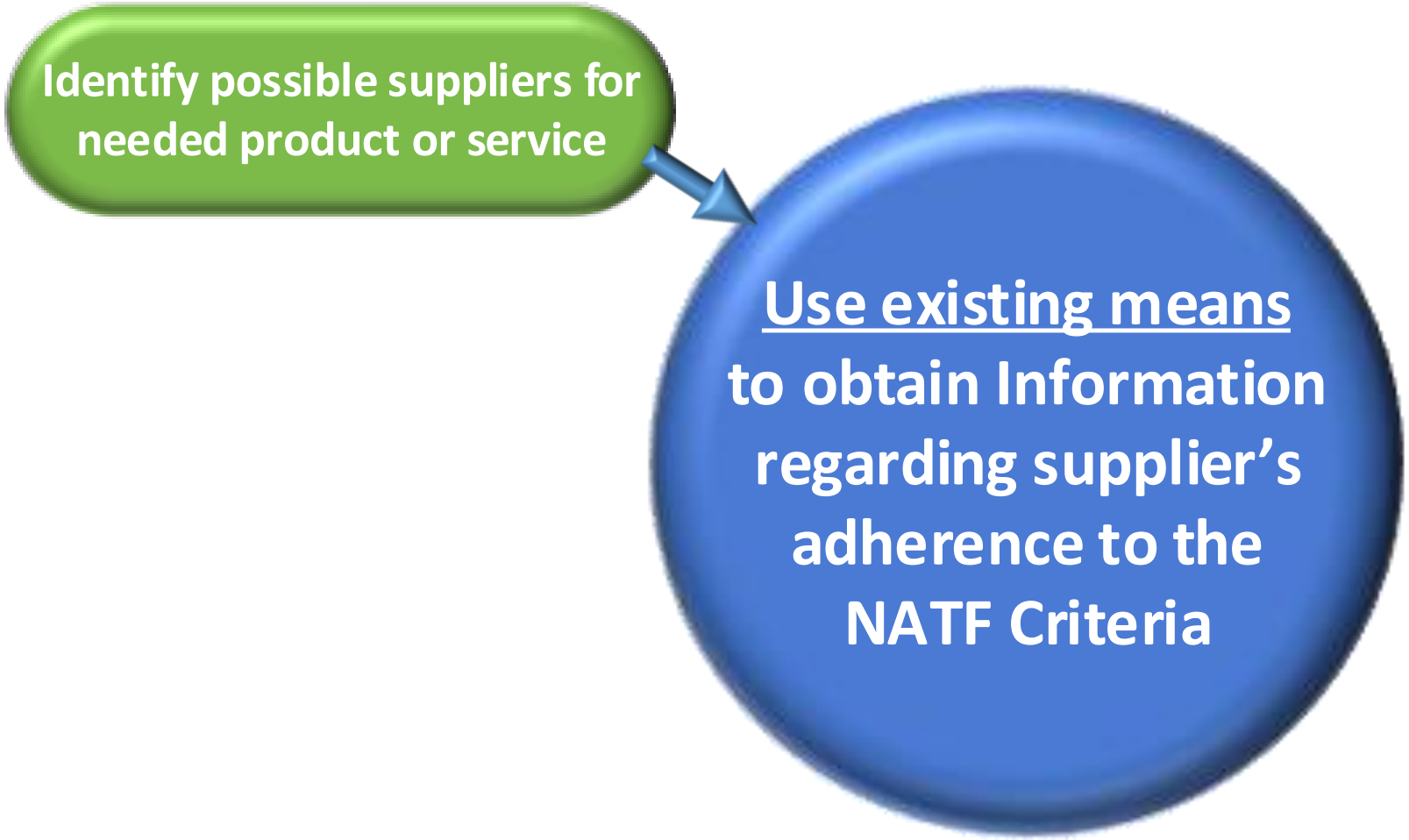
Supplier Cyber Security Assessment: Evaluations

Supplier Evaluation

How is a supplier's adherence to criteria verified and reported?

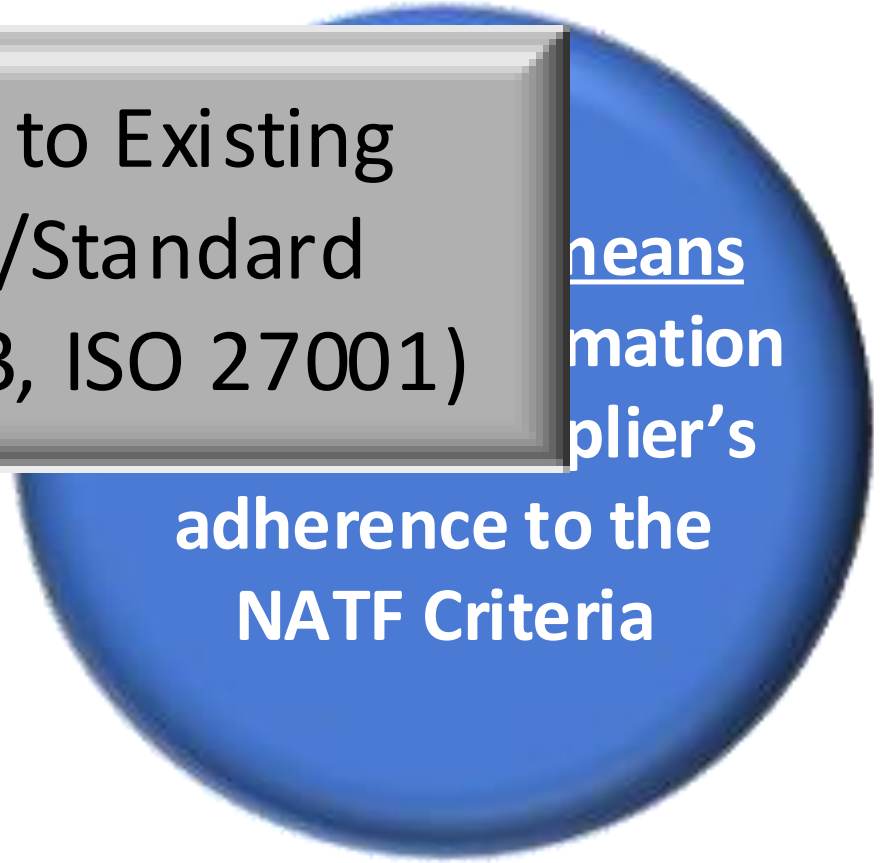
- **Adherence** to the NATF Criteria
  - What is the Supplier's level of adherence to the NATF Criteria for the product or service to be purchased
- **Assurance** for information provided
  - What level of assurance is provided for supplier's information/responses and is the level of confidence appropriate for the product or service to be purchased
- **Address** identified risks
  - Mitigate (either the entity or supplier) or
  - Determine if risk can or must be accepted; document rationale

Obtain Information on Supplier's Adherence

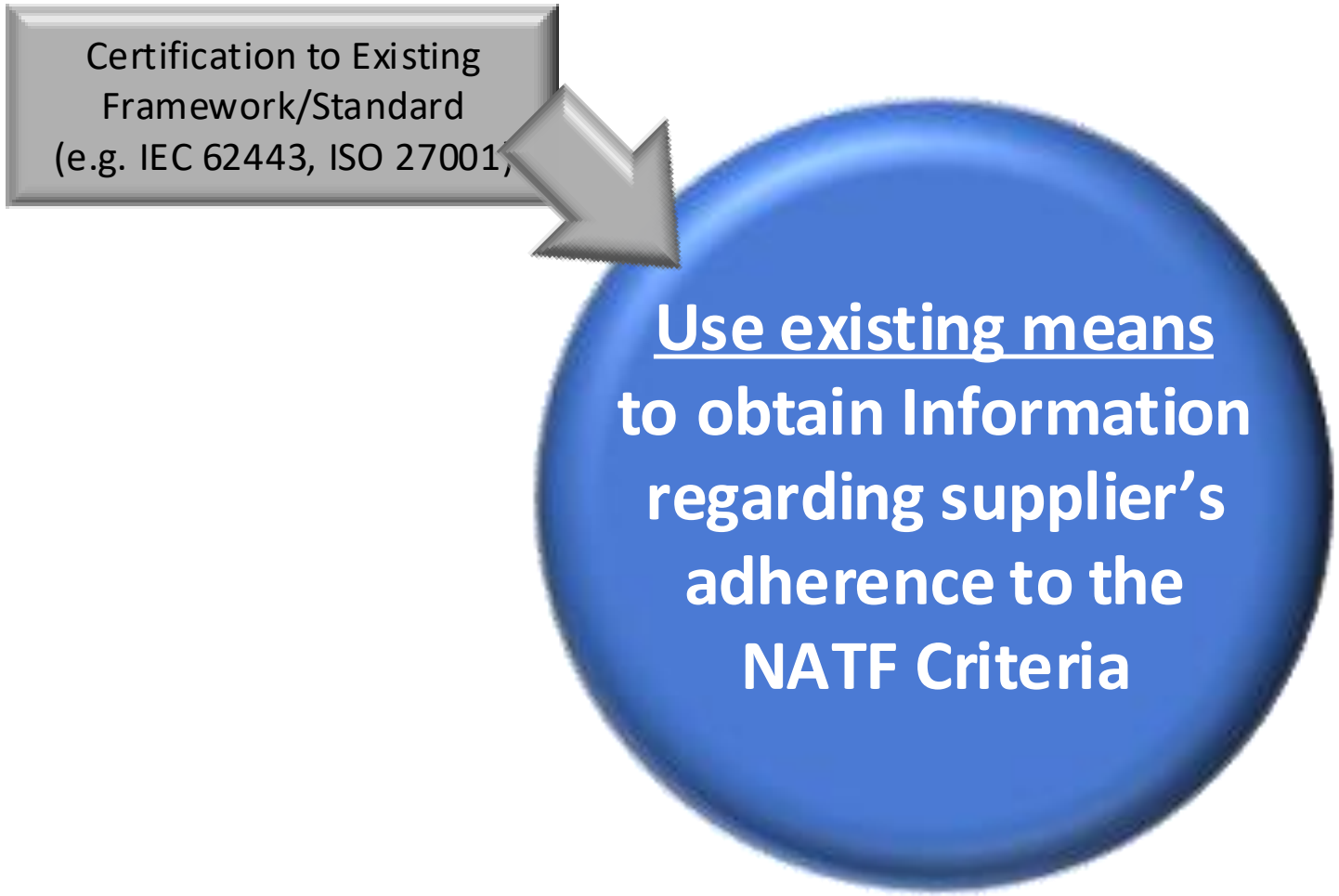


Obtain Information on Supplier's Adherence

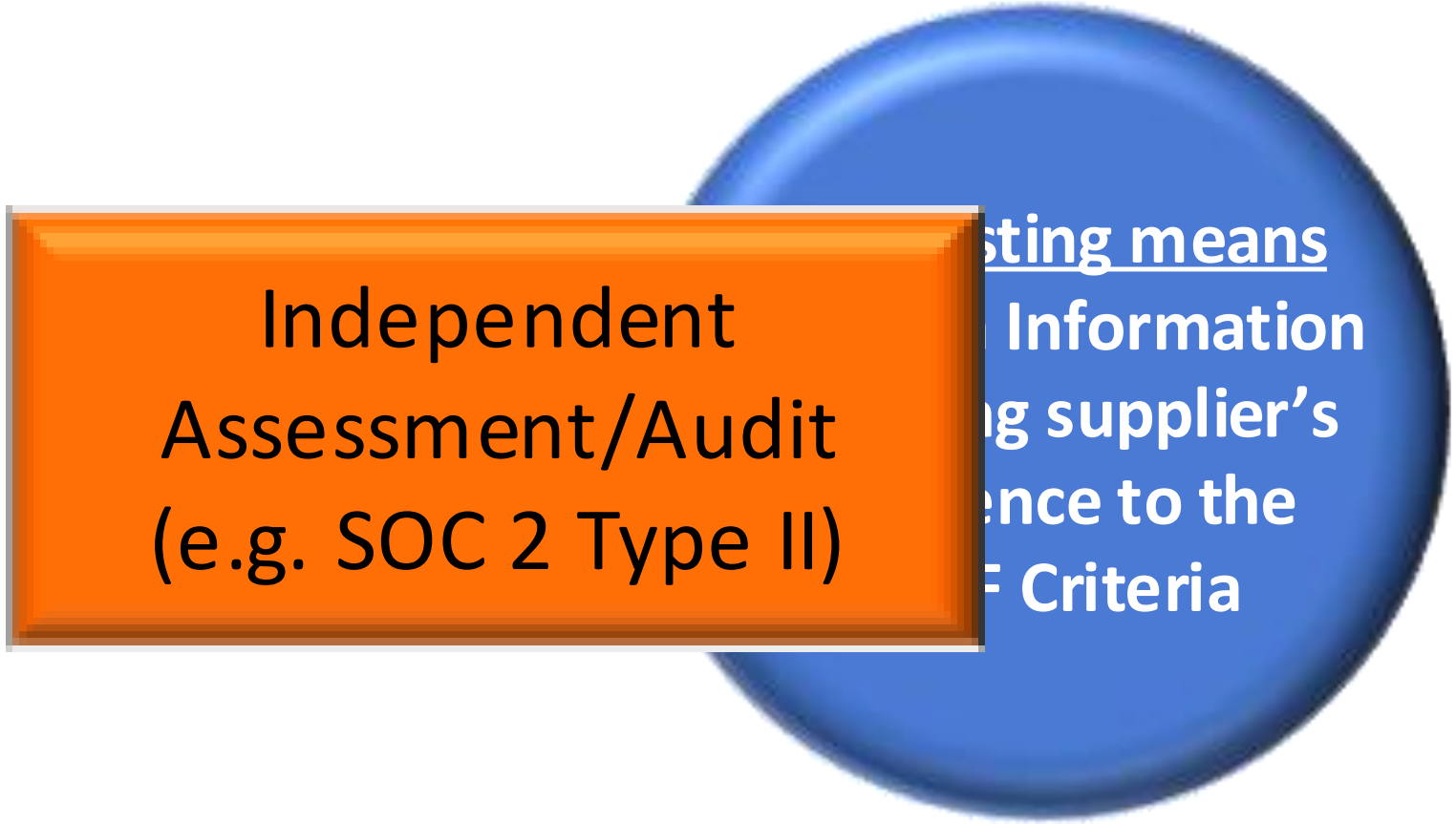
Certification to Existing Framework/Standard (e.g. IEC 62443, ISO 27001)



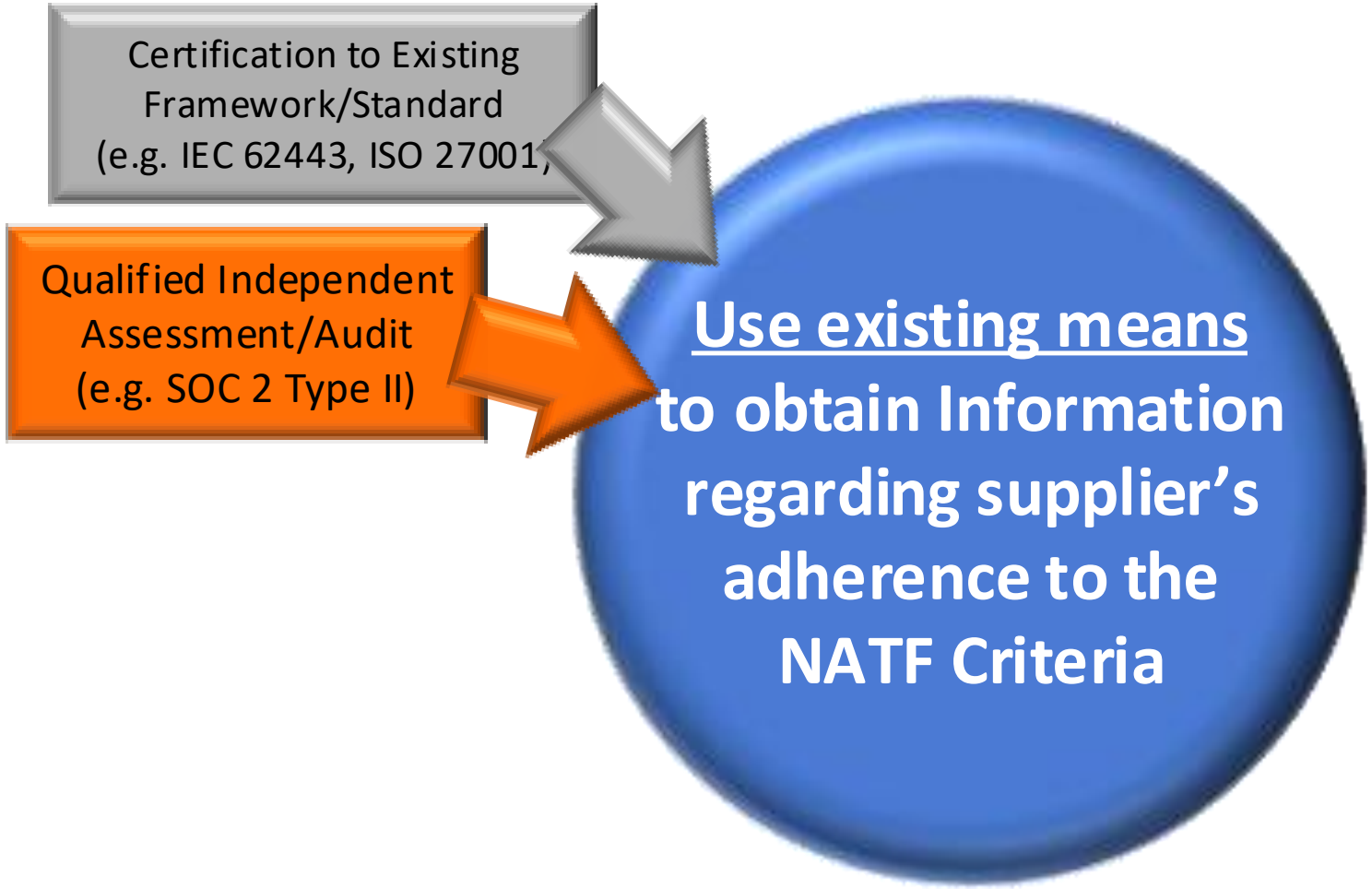
Obtain Information on Supplier's Adherence



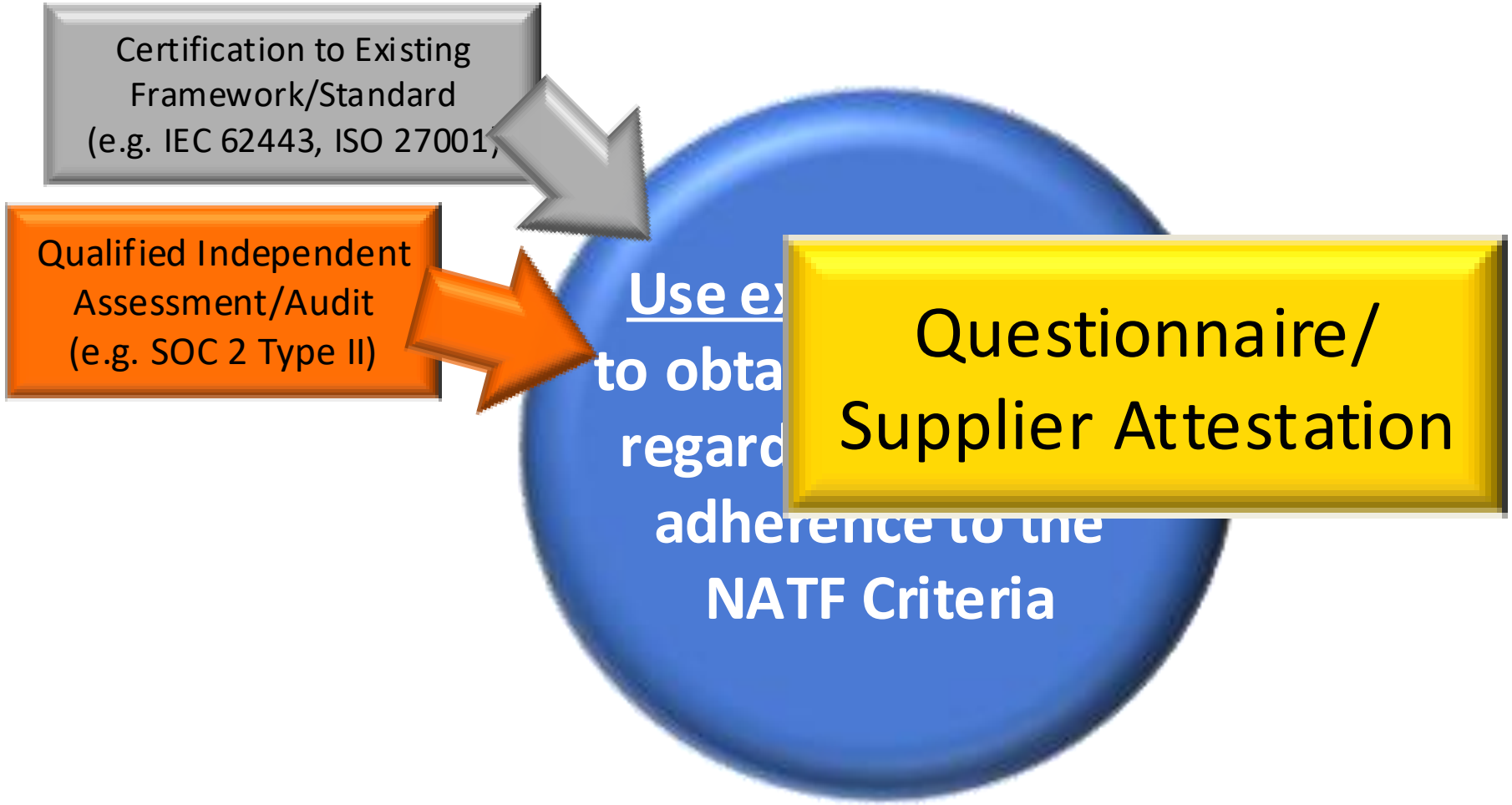
Obtain Information on Supplier's Adherence



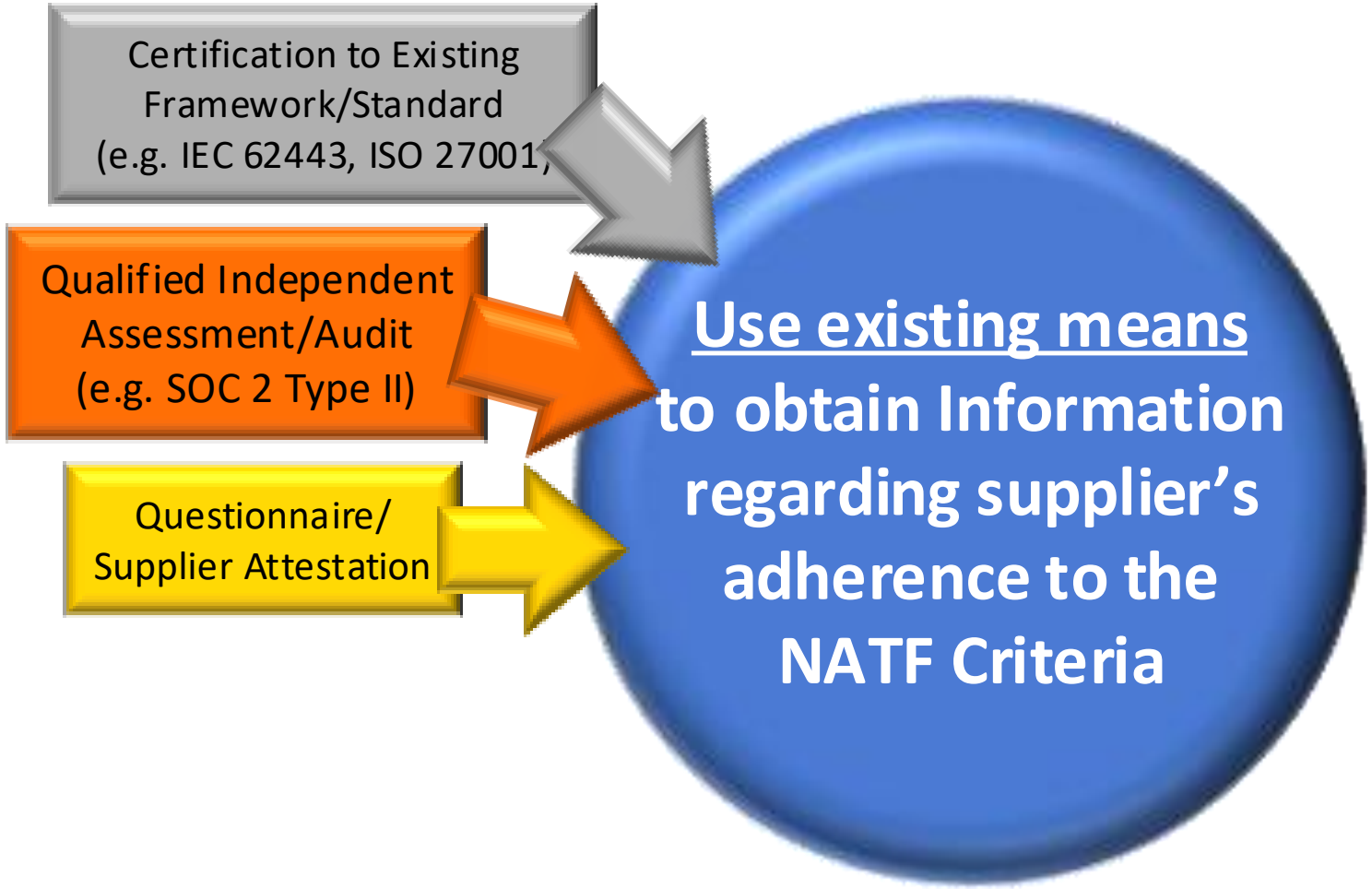
Obtain Information on Supplier's Adherence



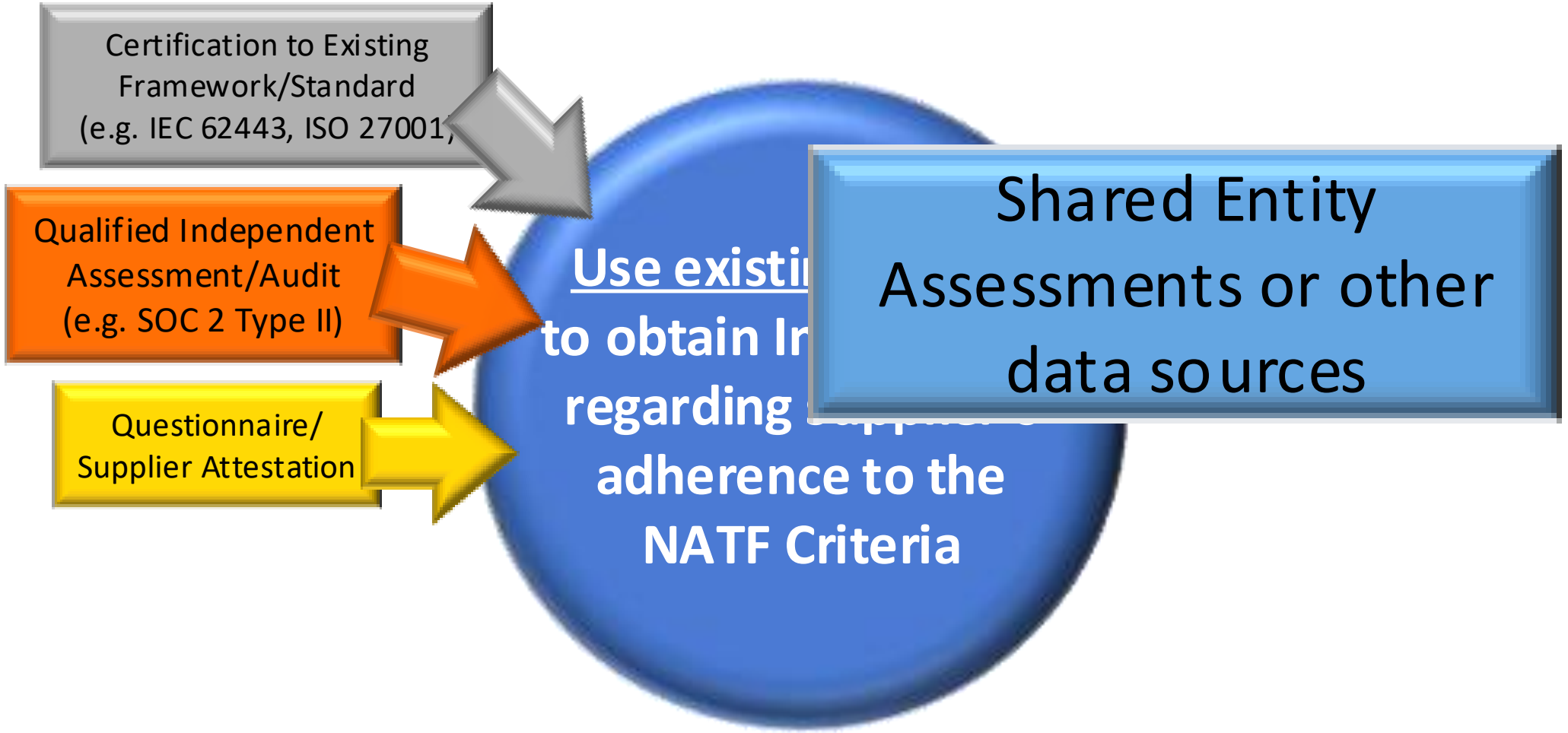
Obtain Information on Supplier's Adherence



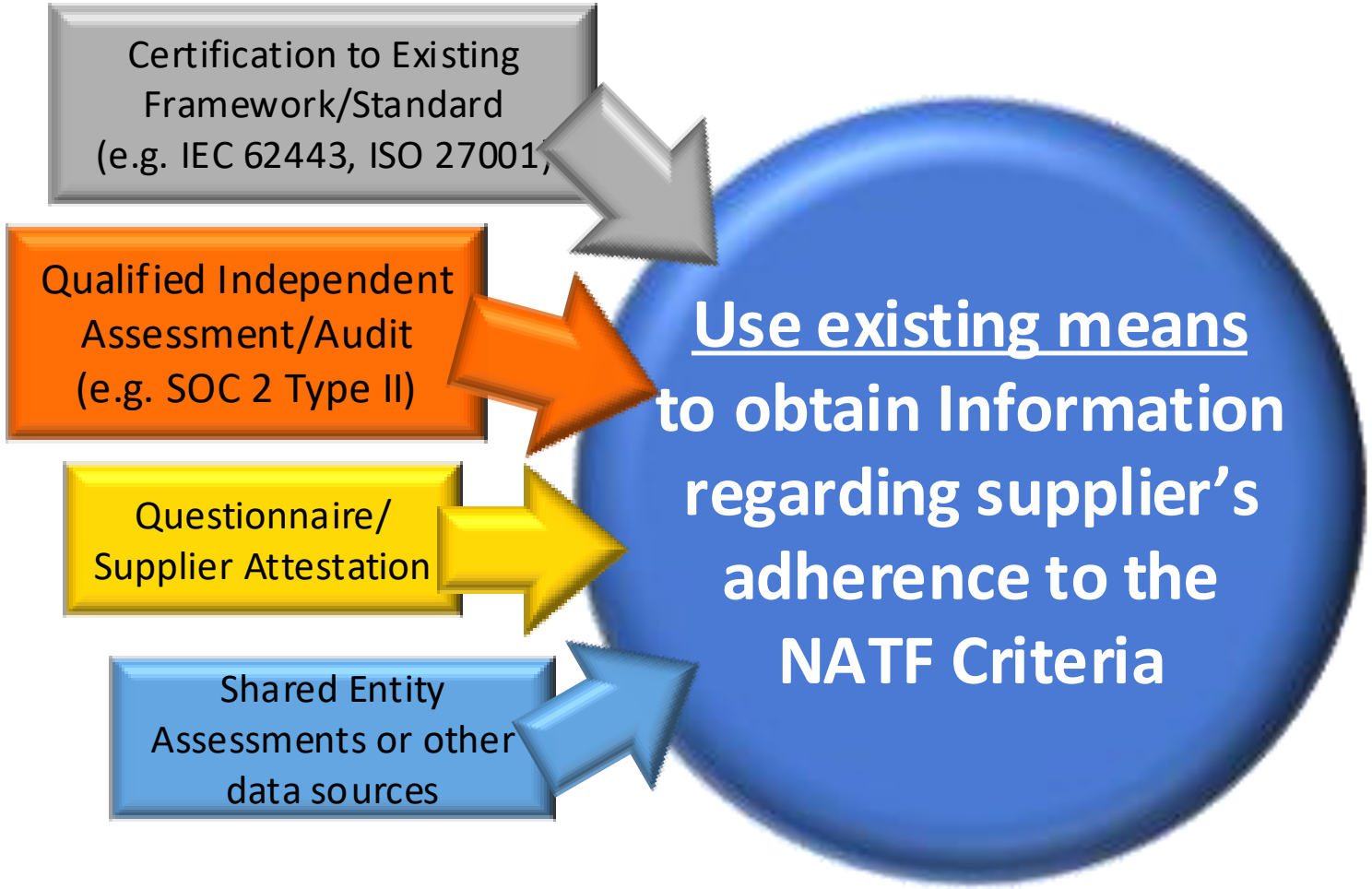
Obtain Information on Supplier's Adherence



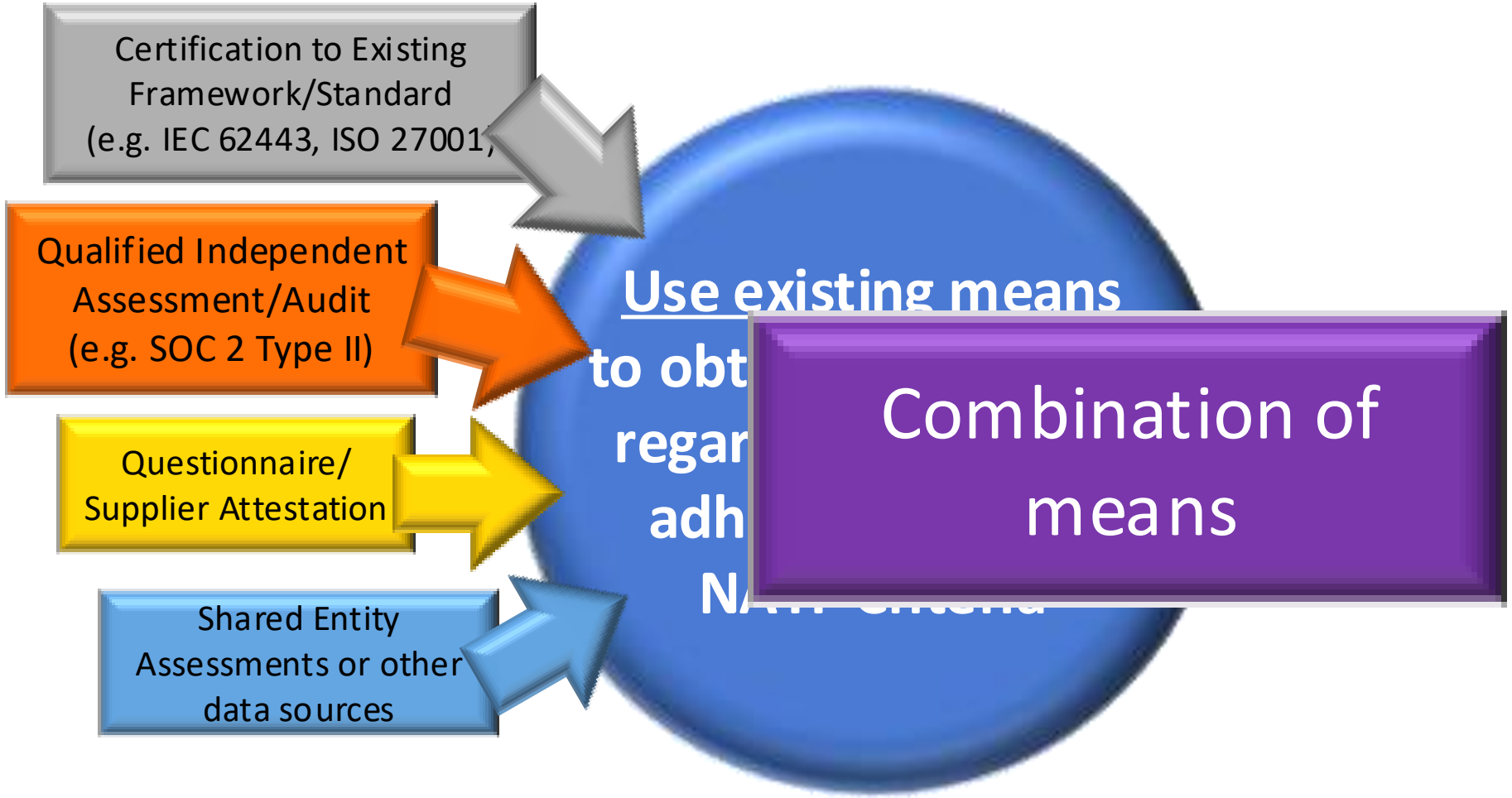
Obtain Information on Supplier's Adherence



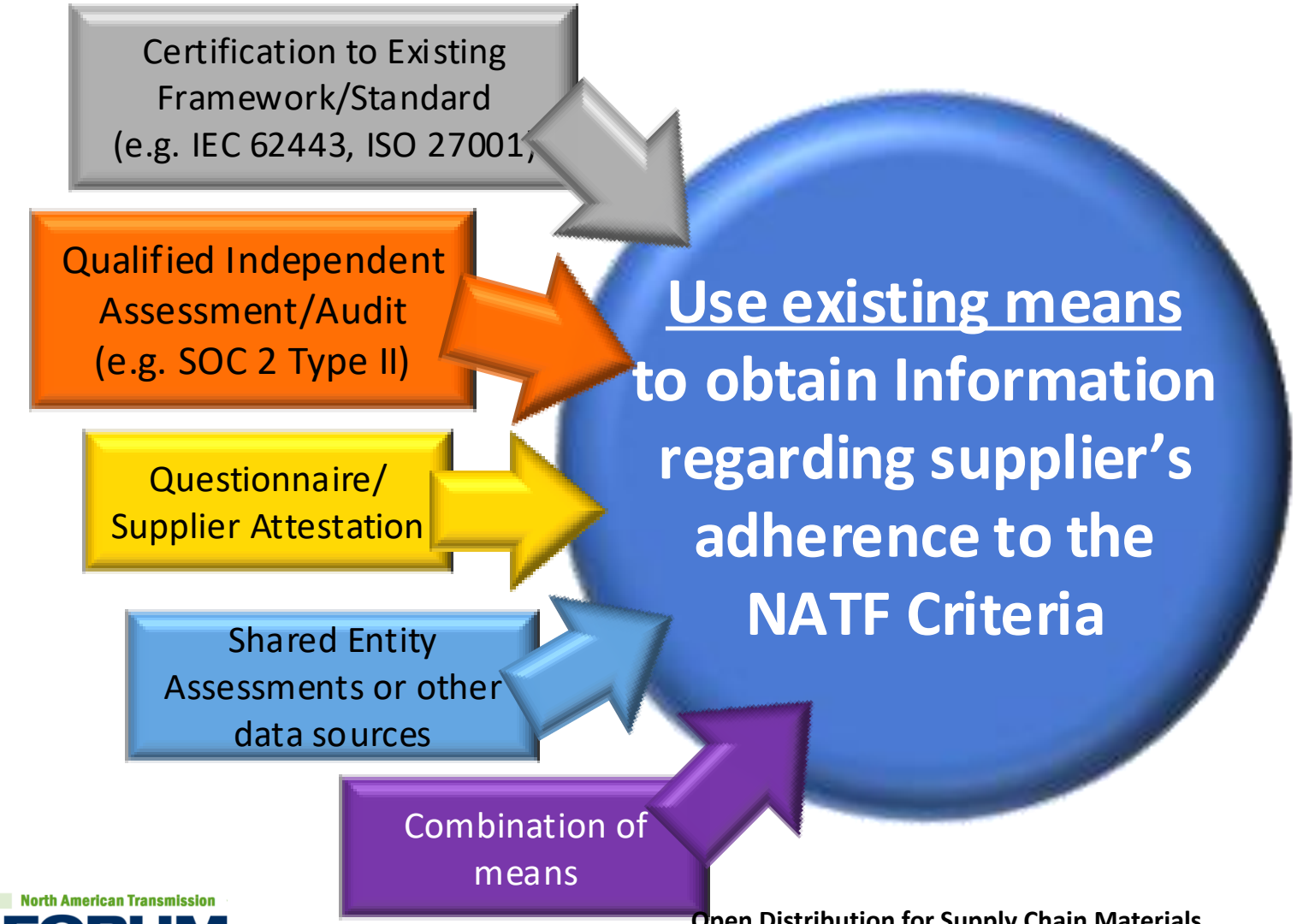
Obtain Information on Supplier's Adherence



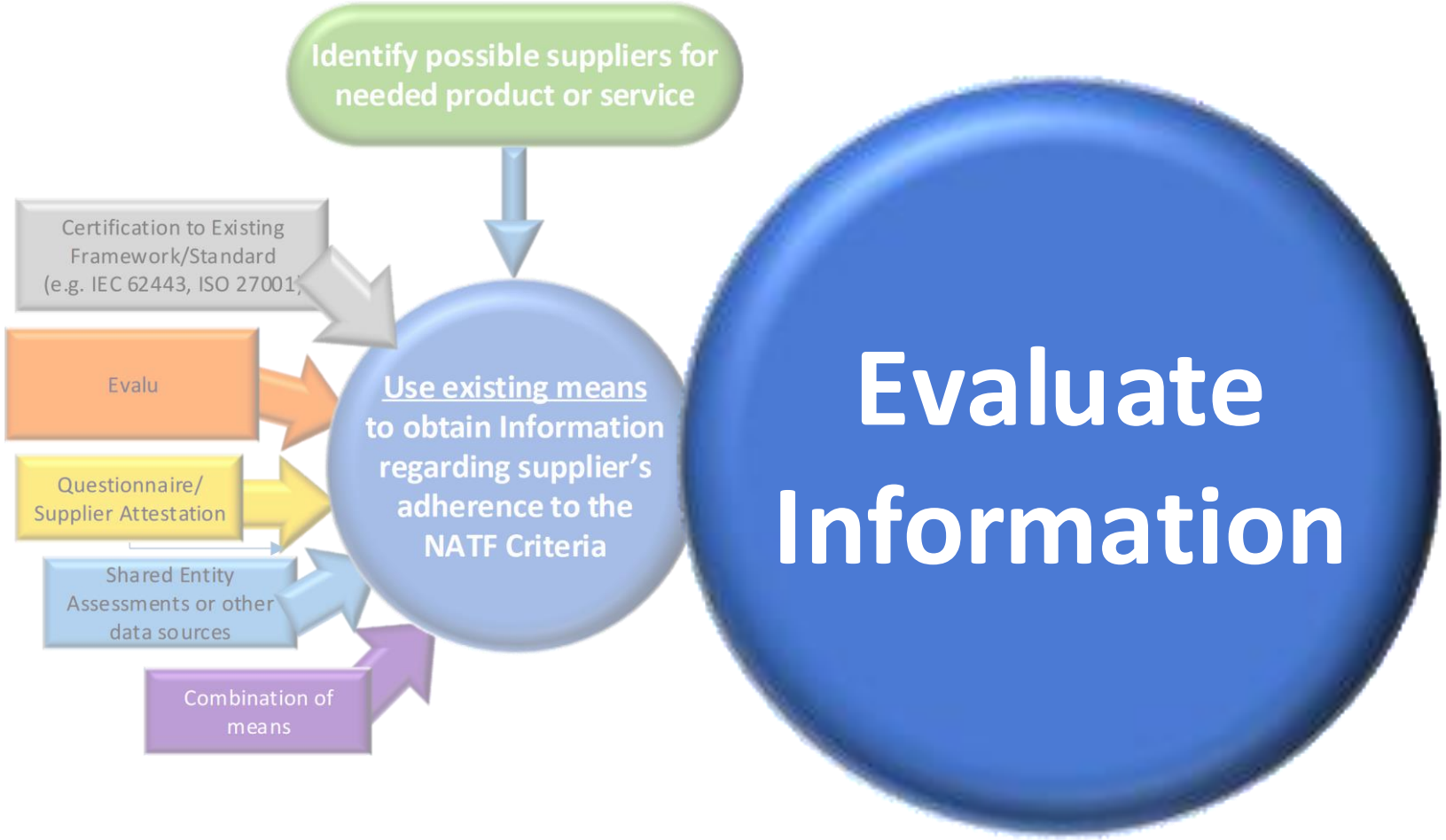
Obtain Information on Supplier's Adherence



Obtain Information on Supplier's Adherence

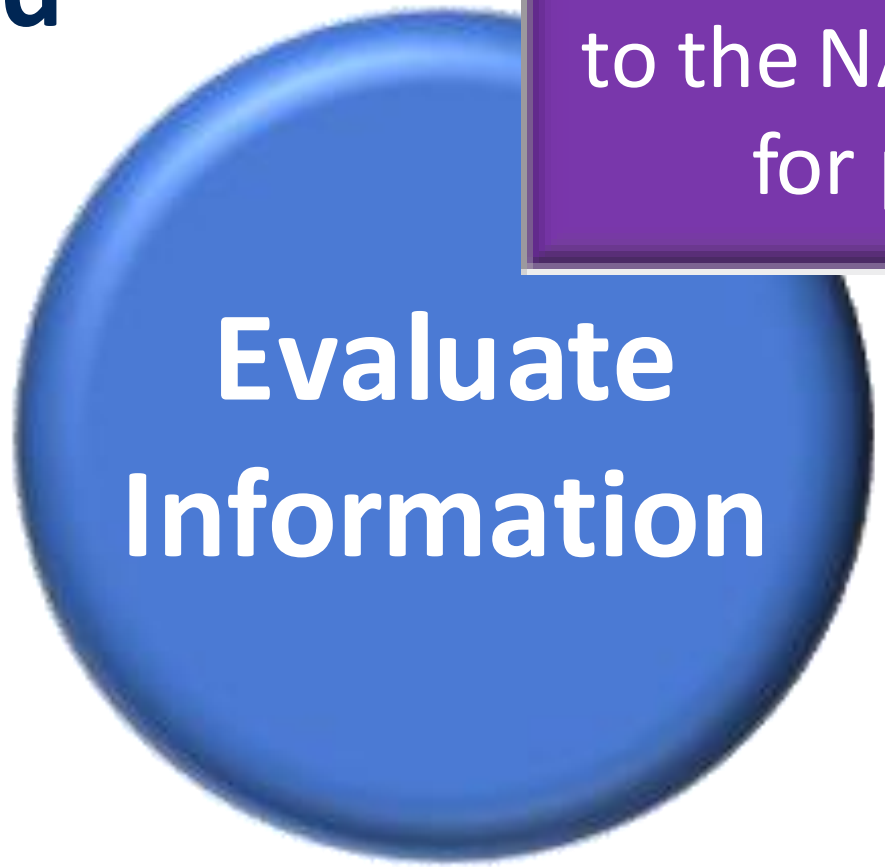


Evaluate the Information Obtained



Evaluate the Information Obtained

Is Supplier's **level of adherence** to the NATF Criteria appropriate for product or service?

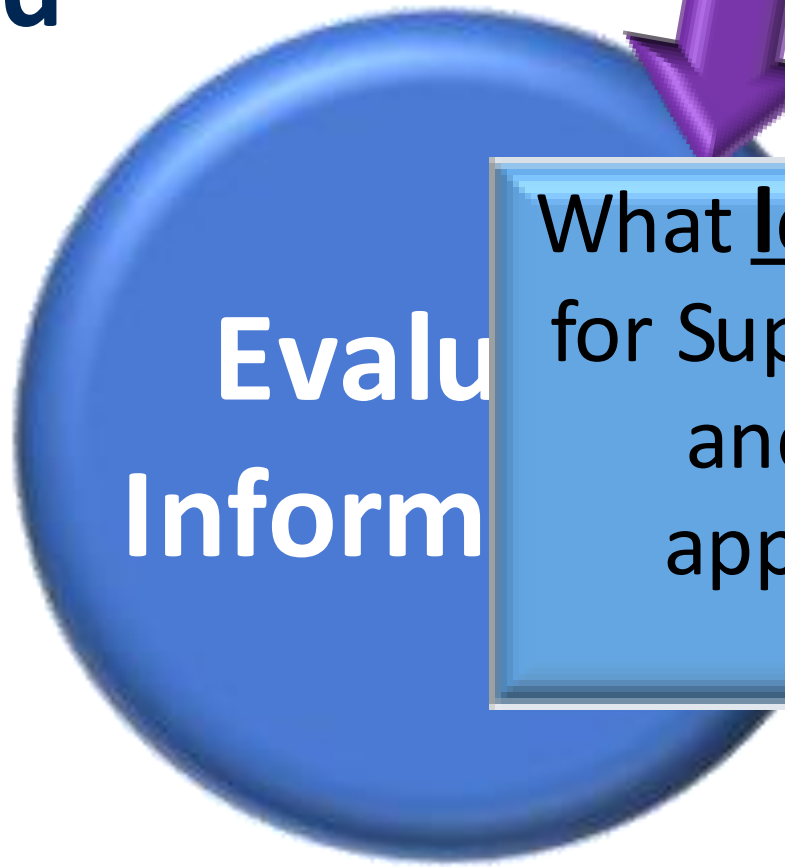


Evaluate the Information Obtained

Is Supplier's **level of adherence** to the NATF Criteria appropriate for product or service?

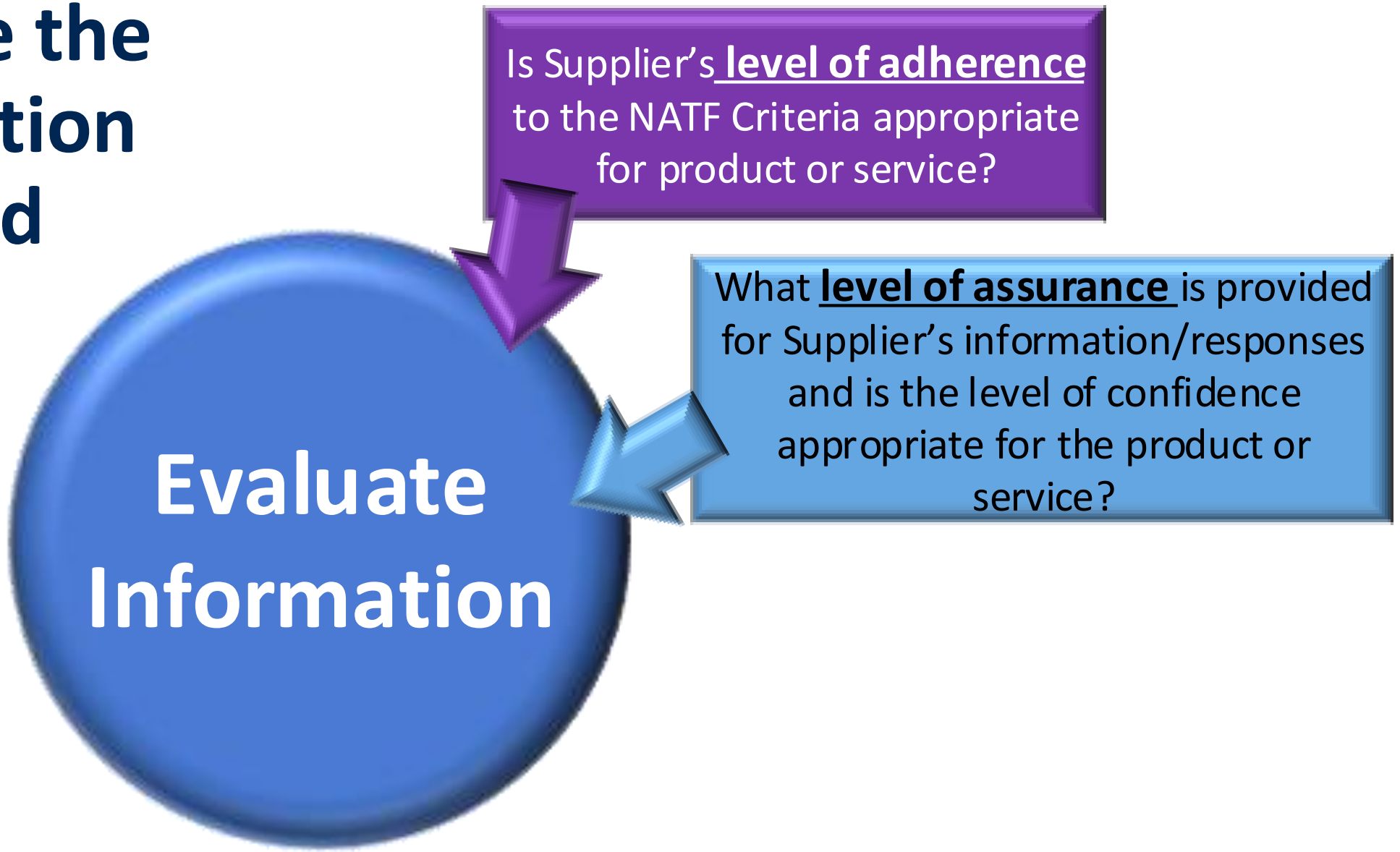
Evaluate the Information Obtained

Is Supplier's **level of adherence** to the NATF Criteria appropriate for product or service?

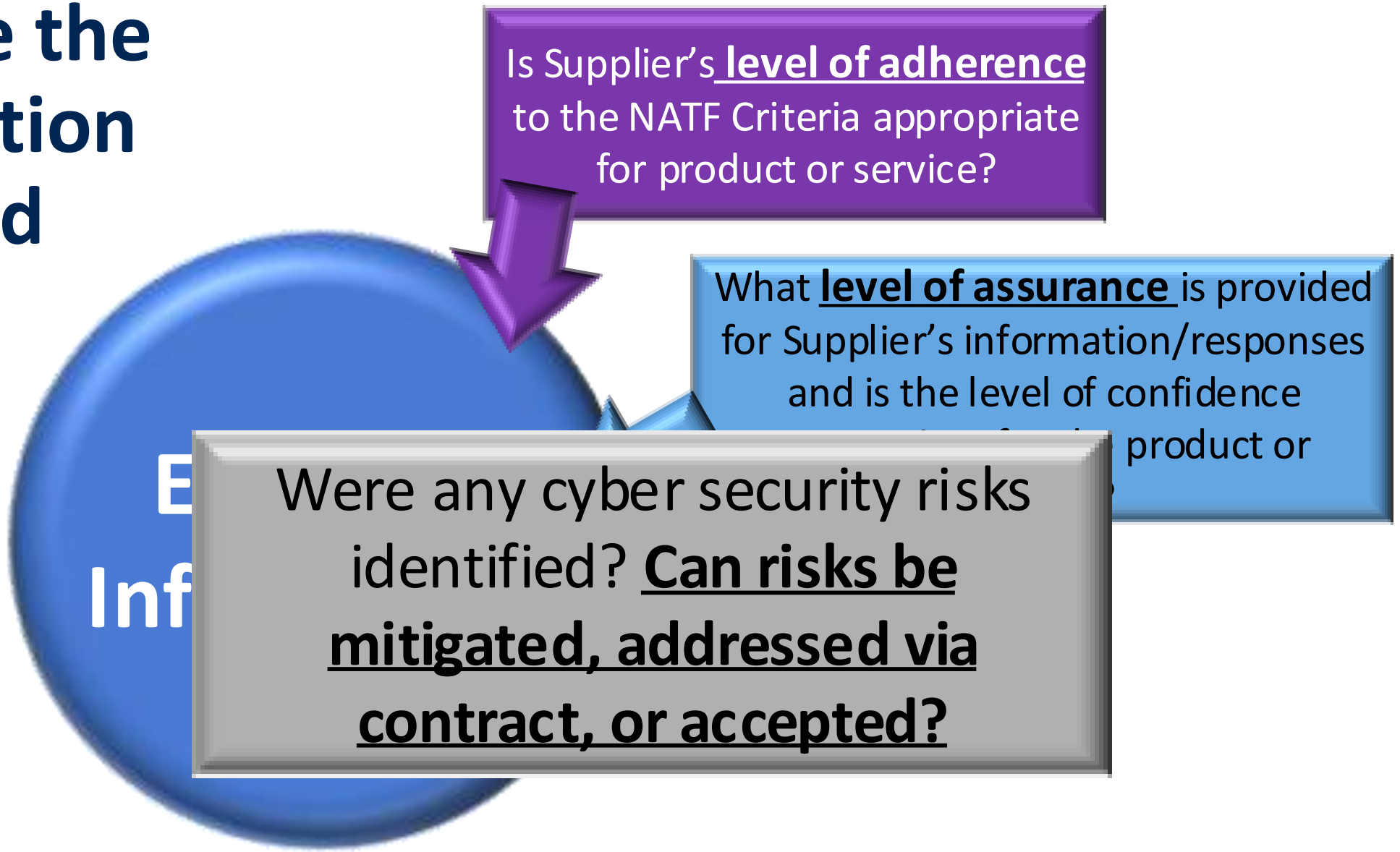


What **level of assurance** is provided for Supplier's information/responses and is the level of confidence appropriate for the product or service?

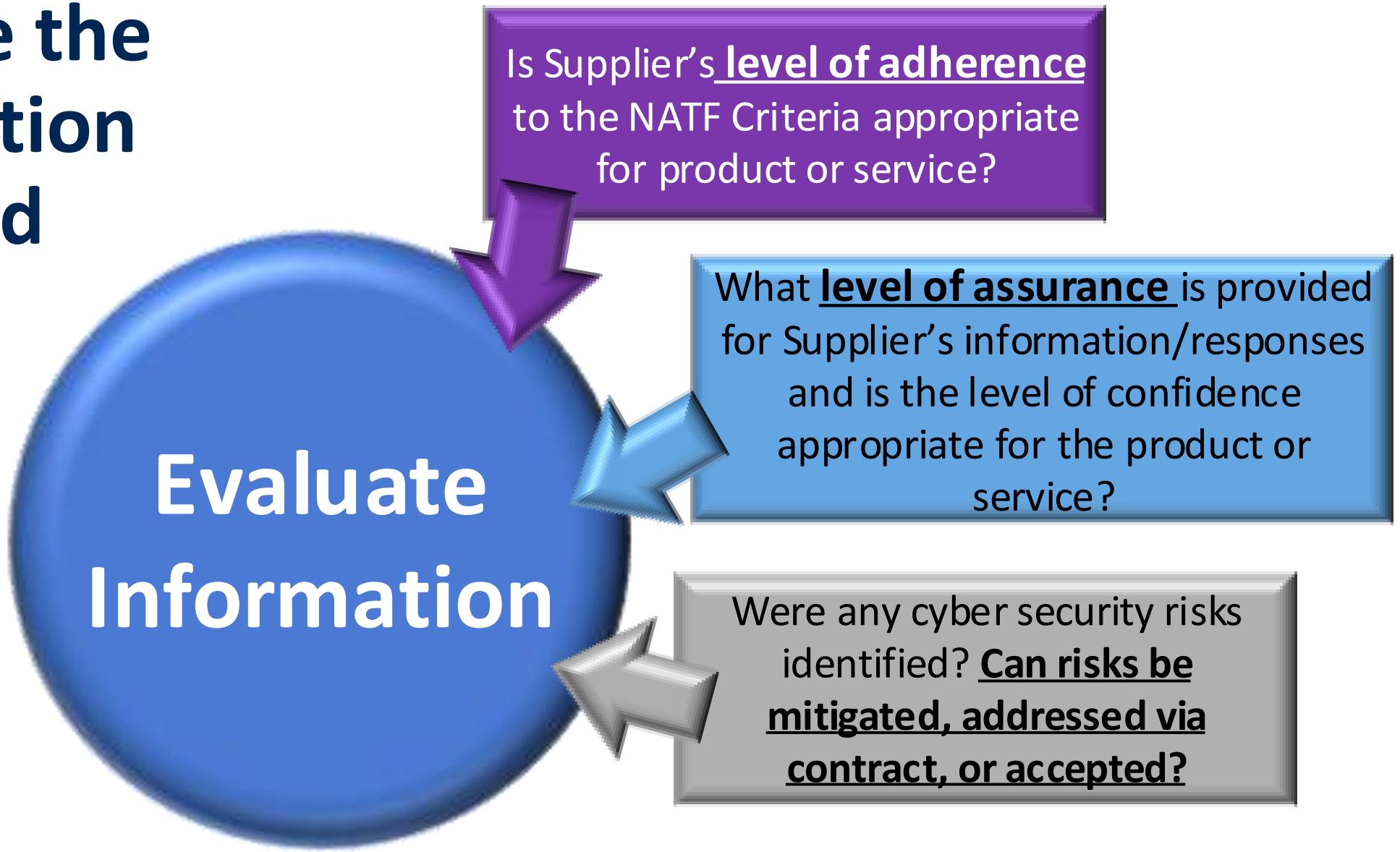
Evaluate the Information Obtained



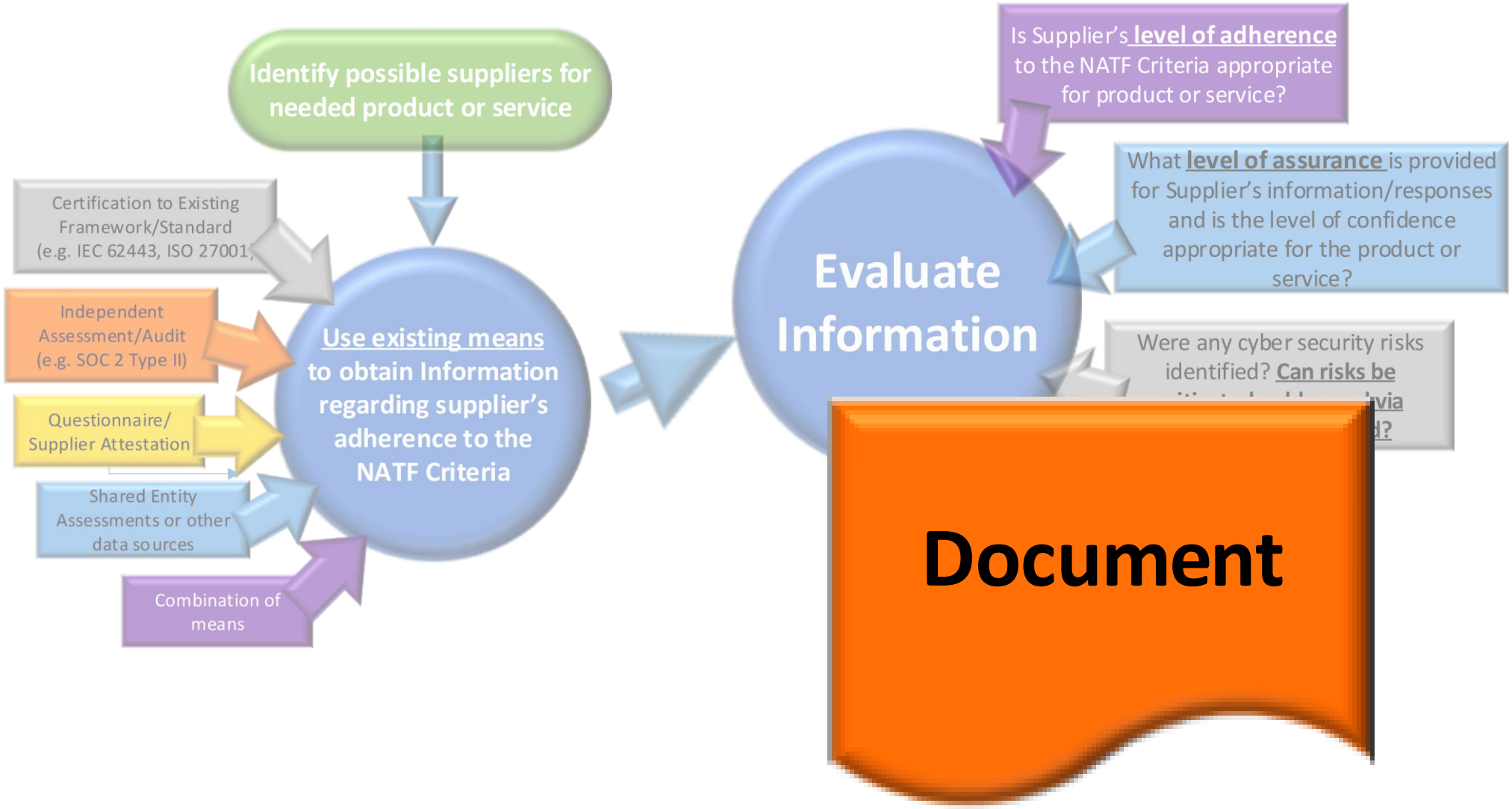
Evaluate the Information Obtained



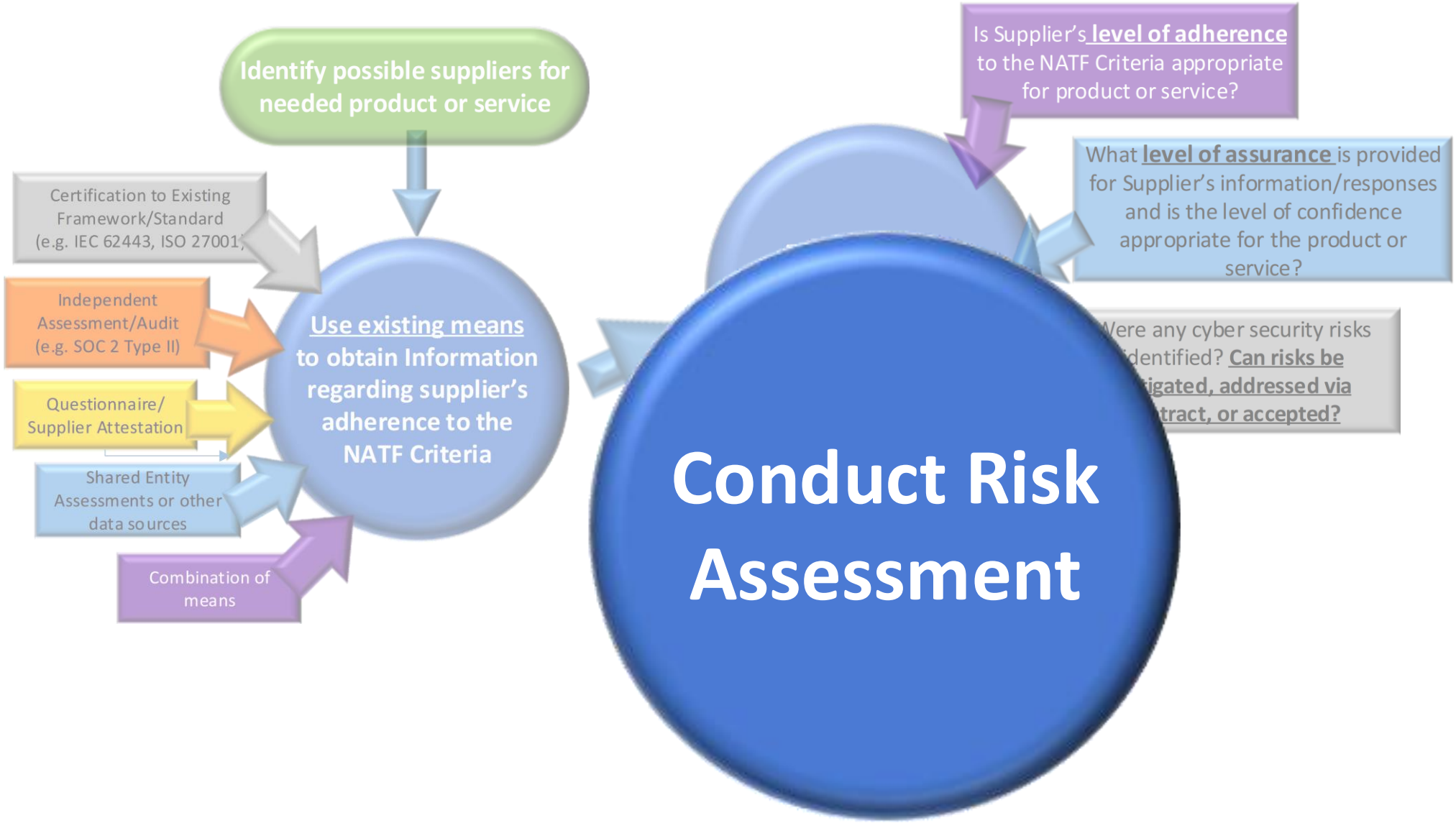
Evaluate the Information Obtained



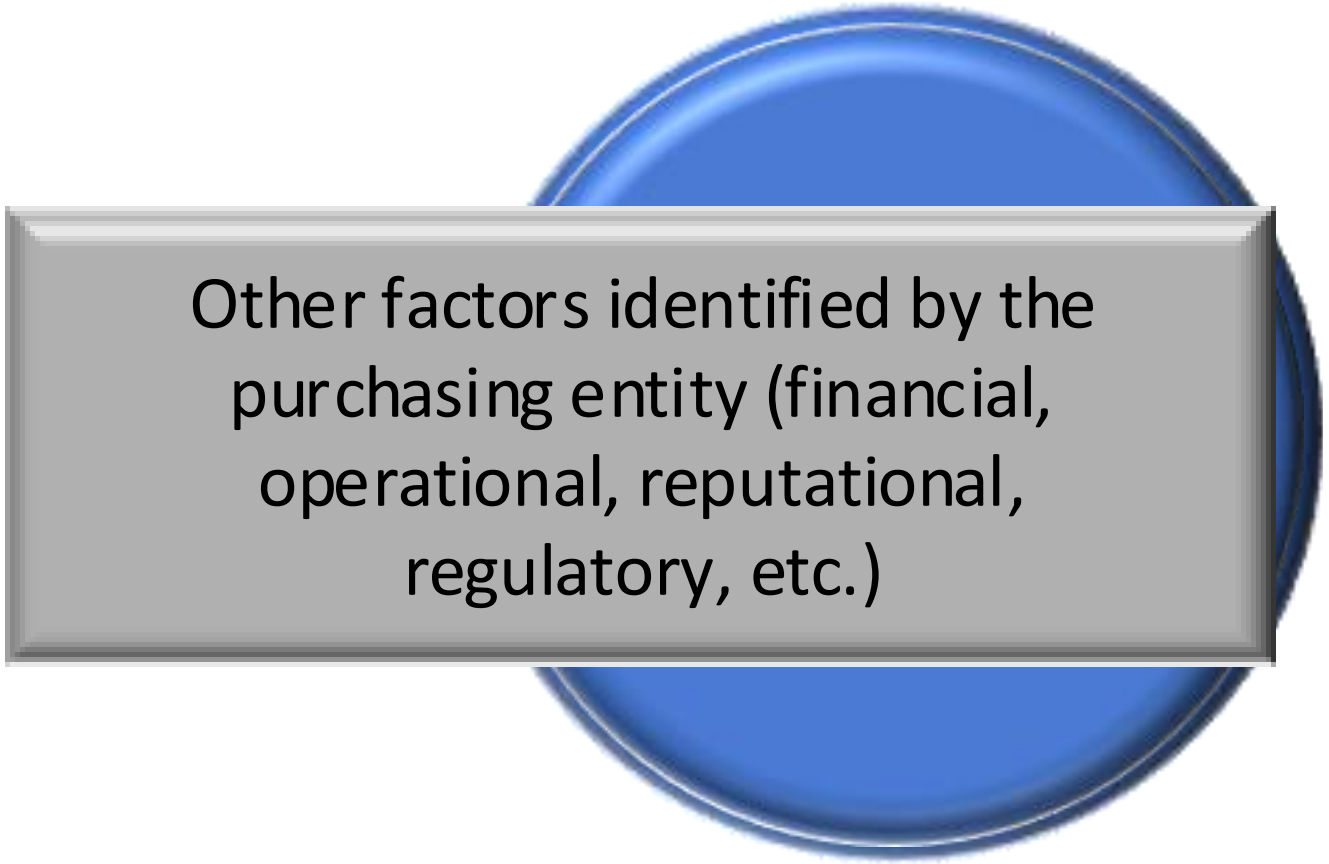
Document!


Identify possible suppliers for needed product or service
Certification to Existing Framework/Standard (e.g. IEC 62443, ISO 27001)
Independent Assessment/Audit (e.g. SOC 2 Type II)
Questionnaire/ Supplier Attestation
Shared Entity Assessments or other data sources
Combination of means
Use existing means to obtain Information regarding supplier's adherence to the NATF Criteria
Evaluate Information
Is Supplier's level of adherence to the NATF Criteria appropriate for product or service?
What level of assurance is provided for Supplier's information/responses and is the level of confidence appropriate for the product or service?
Were any cyber security risks identified? Can risks be
Document

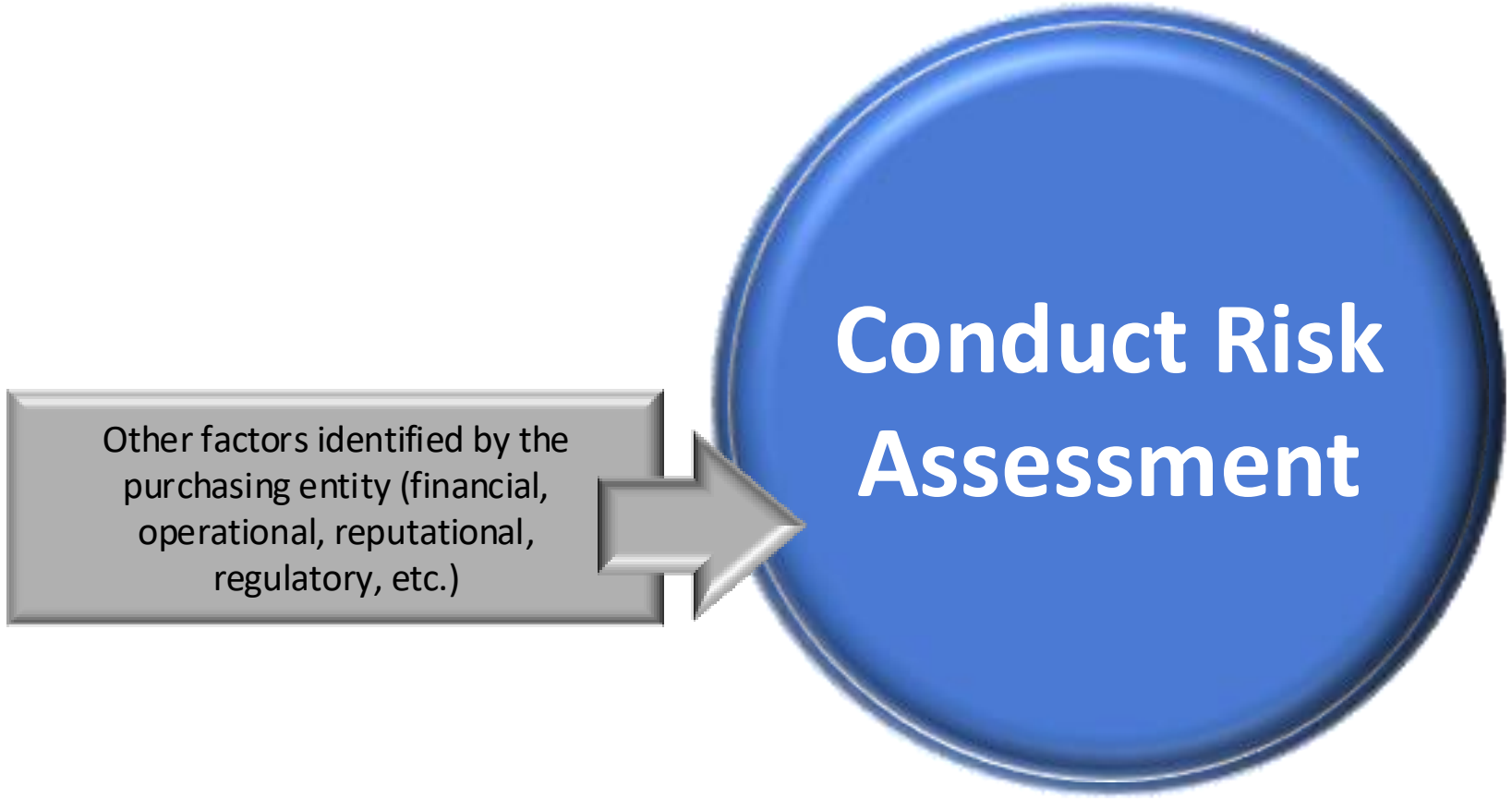
Conduct Risk Assessment



Conduct Risk Assessment

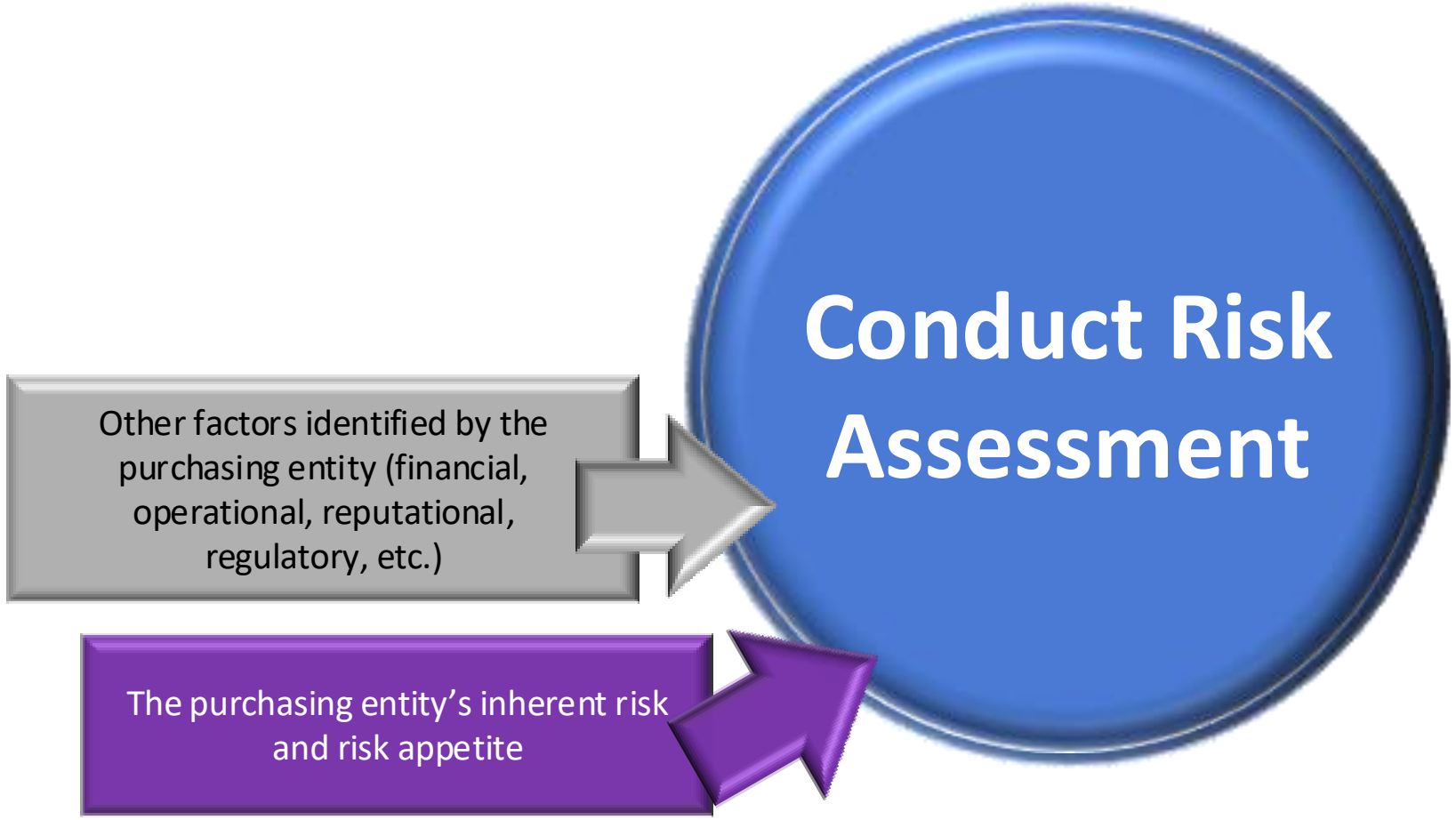


Conduct Risk Assessment

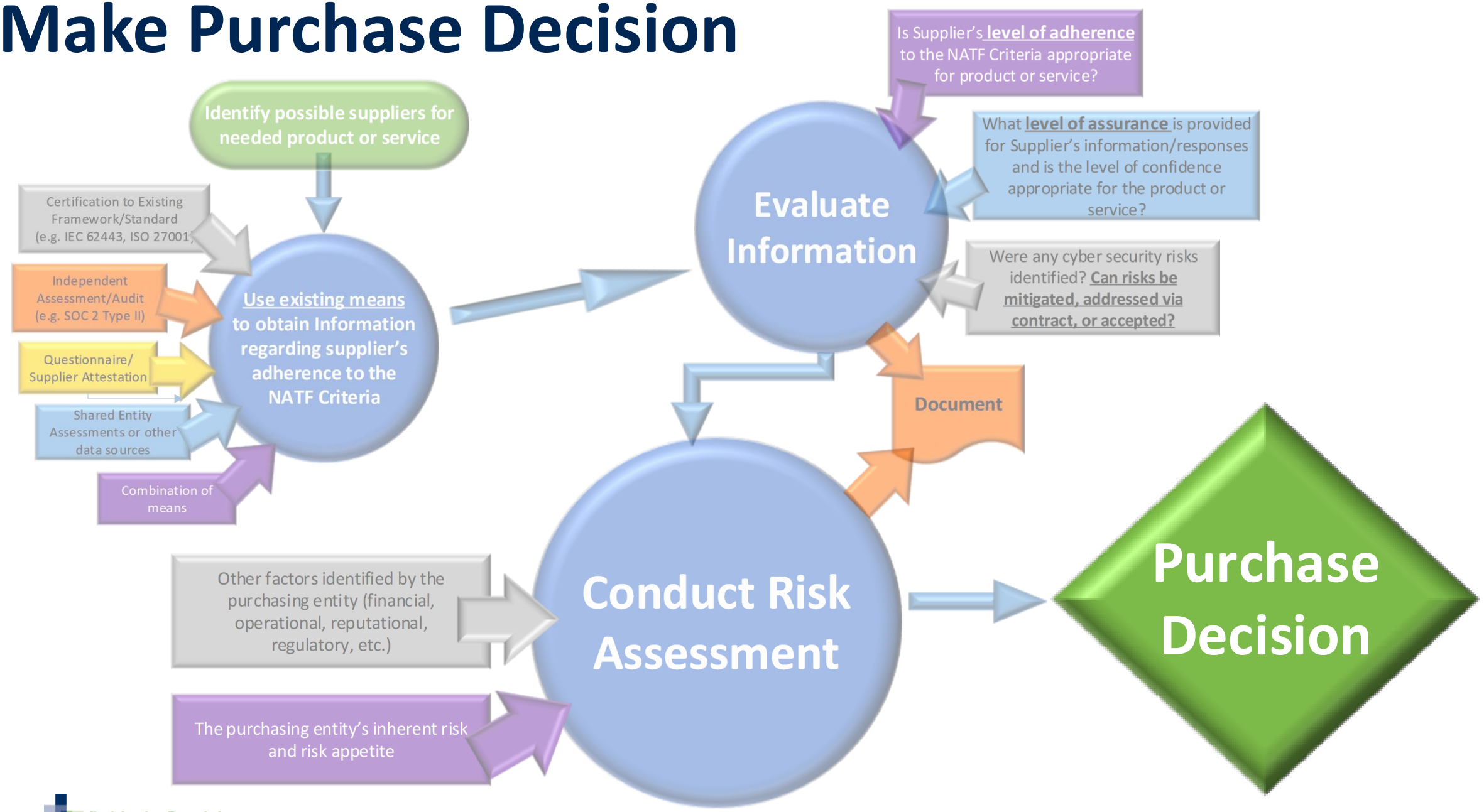


Conduct Risk Assessment

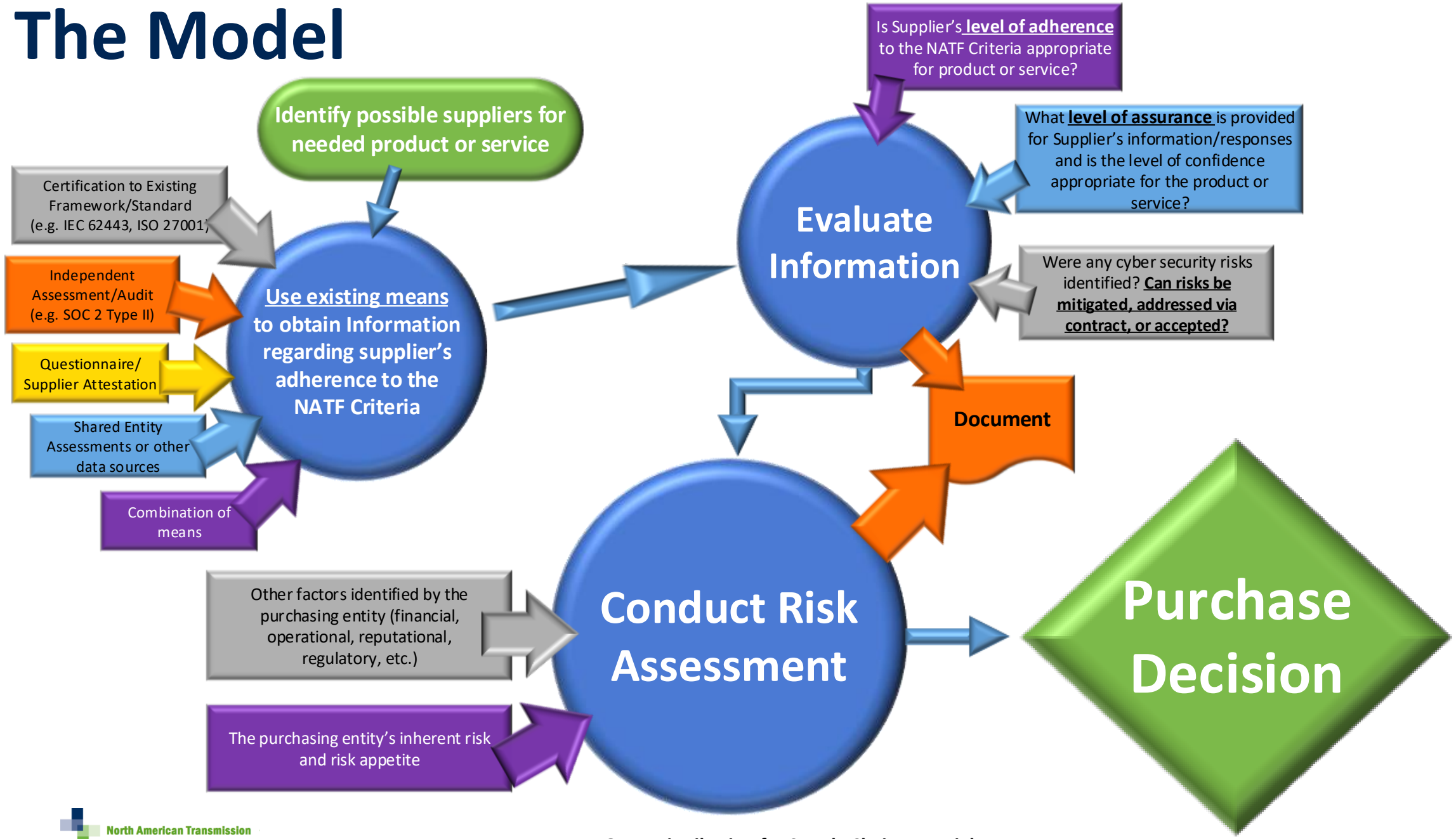
Conduct Risk Assessment



Make Purchase Decision



The Model


Identify possible suppliers for needed product or service
Certification to Existing Framework/Standard (e.g. IEC 62443, ISO 27001)
Independent Assessment/Audit (e.g. SOC 2 Type II)
Questionnaire/ Supplier Attestation
Shared Entity Assessments or other data sources
Combination of means
Use existing means to obtain Information regarding supplier's adherence to the NATF Criteria
Is Supplier's level of adherence to the NATF Criteria appropriate for product or service?
What level of assurance is provided for Supplier's information/responses and is the level of confidence appropriate for the product or service?
Evaluate Information
Were any cyber security risks identified? Can risks be mitigated, addressed via contract, or accepted?
Document
Other factors identified by the purchasing entity (financial, operational, reputational, regulatory, etc.)
The purchasing entity's inherent risk and risk appetite
Conduct Risk Assessment
Purchase Decision

The Model – A Supplier Perspective

Rob Koziy, OSI

Problem statement:

- *NERC Entities are required to complete security risk assessments of multiple critical suppliers in a very short timeframe*
- *Many entities do not have the resources to conduct extensive on-site audits or develop lengthy security questionnaires*
- *Suppliers are challenged to support large numbers of on-site entity audits & customized security questionnaires*

The Model – A Supplier Perspective

1. The “every entity for themselves” approach will cause delayed responses and require the reassignment of significant supplier resources to support entity on-site audits, customized security questionnaire responses, and contract review by legal teams

2. The common NATF criteria combined with security data sharing sites such as EPRI and A2V, enables suppliers to provide detailed security responses about their organization and products to many entities at once

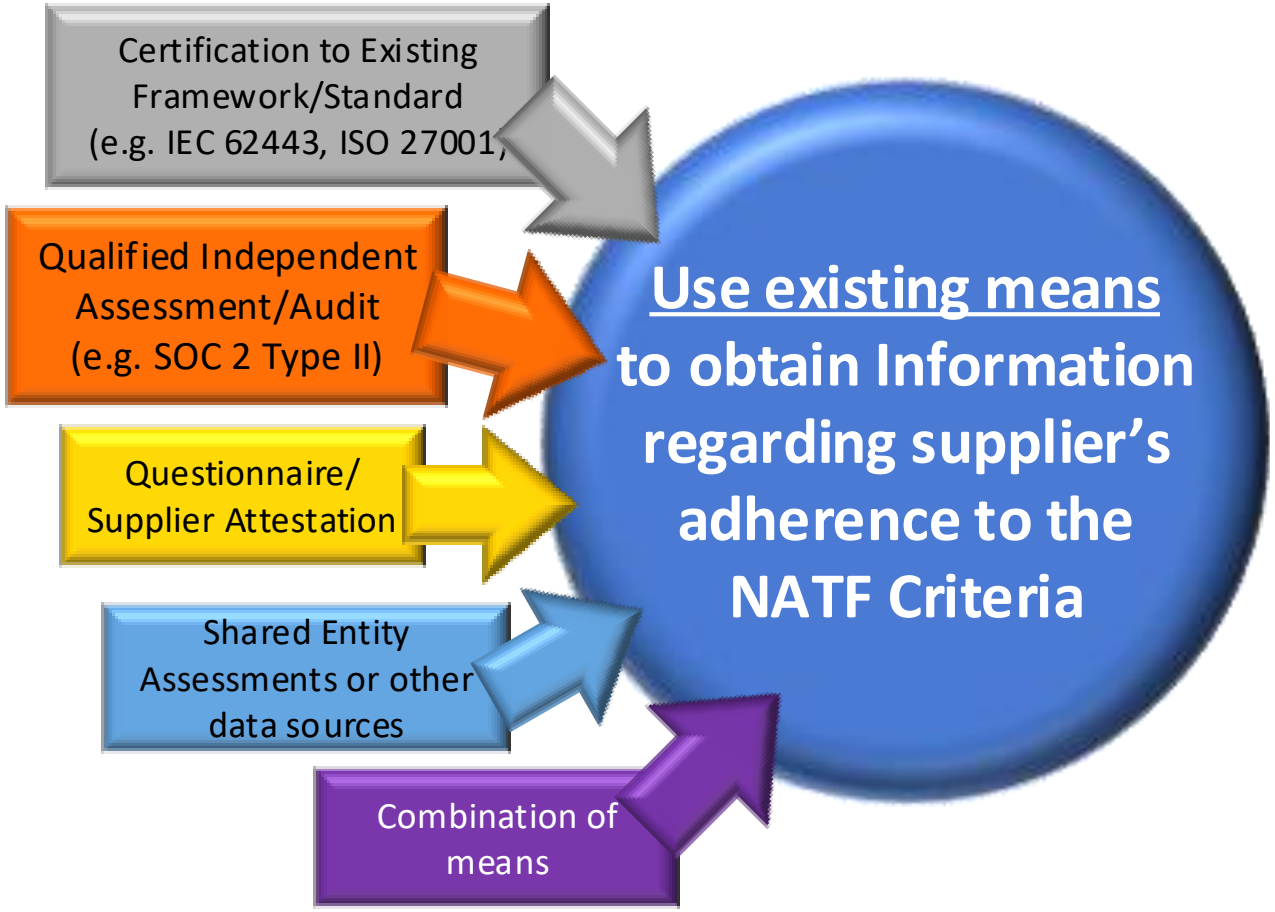
3. Entities that review supplier information posted in the common NATF criteria format, and use EEI contract language as a baseline, will significantly reduce the burden on supplier and entity resources to complete their risk assessment

4. Entity review of a supplier’s independent audit and/or assessment reports (if available) enables the entity to gain critical insights of the security controls used by the supplier, in order to focus on risk areas that require further discussion, additional contract language, or a narrowly focused on-site audit by the entity

5. Use of the NATF, EEI, EPRI & A2V tools is a win-win for suppliers, entities and the industry

The Model - Supplier Evaluations

Matthew Barbera, Deloitte



There are many ways to obtain information regarding a supplier's cyber security practices using the NATF Criteria.

North American Transmission FORUM

The Questionnaire

Tony Eddleman, NPPD

Coming Soon!

North American Transmission FORUM

The EEI Procurement Language

Kegan Gerard, EEI

For further explanation, see the "Supplier Cyber Security Assessment Model" Document

The EEI Procurement Language

- Supplier investigations are one piece of puzzle – procurement contract language provide an additional piece
- *Model Procurement Contract Language Addressing cybersecurity Supply Chain Risk*
  - Original focus was CIP-013 R1.2
  - Offers a starting point or temperature check
- Update discussions underway
- Email SupplyChain@eei.org to provide input

North American Transmission FORUM

Implementation Resources and Tools

Disclaimer:

Implementation of the Model

- Tools are being developed that can assist entities and suppliers in sharing supplier information
  - Locating supplier data
    - Adherence to NATF Criteria (at various levels of assurance)
    - Responses to the Questionnaire
    - Shared Assessments
  - Streamlining Risk Assessments
  - Organization of Data

Vendor Organization – A2V

Fortress/AEP Asset to Vendor (A2V) Product

- Alex Santos, CEO and Co-Founder

Asset to Vendor (A2V) Overview

Mission: Secure the utility industry's supply chain

Solutions for:

- Utilities – Turnkey program implementation
  - **Library** of completed assessments
  - **Technology** for program management
  - **Services** to augment or fully execute program
- Vendors – Reduced administrative burden
  - **Portal** for securely distributing vendor & product assessments/certifications
  - **Services** to encourage standardization of approaches by clients

Asset to Vendor Specifics

- **Assessment** readiness – 361 CIP-013 identified vendors with completed, validated assessments by May 31
- **Technology** – Tracking activities, demonstrating compliance and out-of-the-box audit reports
- **Patch verification** – Authenticity and integrity validated, hashed and stored in a blockchain
- **Product** assessments – (1) Open/private source intelligence, (2) validated controls and (3) security analysis
- **Services –** Validations, vendor/product background checks, contract reviews and program management
- **Monitoring**
  - Historical and daily alerts for breaches, changes in control and foreign ownership within your supply chain
  - Fourth parties also monitored
- Deployment models
  - On premise or cloud
  - Structured as capital expenditure or operations & maintenance expense
  - Go-lives in under two weeks
  - Stand-alone software, services or a total solution
- Hardware **bill-of-materials** coming in Q3 2020
- Services tailored to meet **CIP-013 compliance**, but also much broader vendor or supply chain **risk management**

See more on AssetToVendor.com

Vendor Organization – EPRI

Electric Power Research Institute Supplier Portal

- Tobias Whitney, Technical Executive, Power Delivery and Utilization – Cyber Security

Supply Chain Security Exchange Explained

- Supplier Security Database (scse.epri.com) will address the following priorities:

Vendor Security Practices

Product Security Features

CIP Compliance Capabilities

Supply Chain Security Exchange Explained

- Supplier Database will address the following priorities:
  - Vendor Info (NATF)
  - Vendor Security Certs & Standards (NATF)
  - Vendor Security Capabilities (CIPC)
    - Open Source Software
    - Risk Management Lifecycle
    - Vendor Risk Management Lifecycle
  - NERC CIP-013 (NERC)
- Product Capabilities
  - NERC CIP Standards (CIP-002 – CIP-013)
  - Provenance (CIPC)
  - Open Source Software (CIPC)
  - Secure Equipment Delivery (CIPC)

- Streamlined Approach to Vendor Product and Capability Research

North American Transmission FORUM

Next Steps

Next Steps

- Continued collaboration across industry
- Socializing Model with suppliers and third-party assessor industries
- Completing current projects
- Addressing implementation issues that arise and creating projects where needed

Communication and Support

- Keep web page updated
- Provide entity assistance, as desired
  - Webinar Series
  - Workshops

North American Transmission FORUM

Q&A

Questions