North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

NATF Supply Chain Implementation Guidance

Ken Keels, Valerie Agnew and Ryan Stewart

March 21, 2022

NATF Members

95 members

87 affiliates

Member Types

IOUs

Federal/Provincial

Cooperatives

State/Municipal

ISOs/RTOs

Coverage (US/Canada)

~85% miles 100 kV+

~90% net peak demand

ERO Endorsement of Implementation Guidance

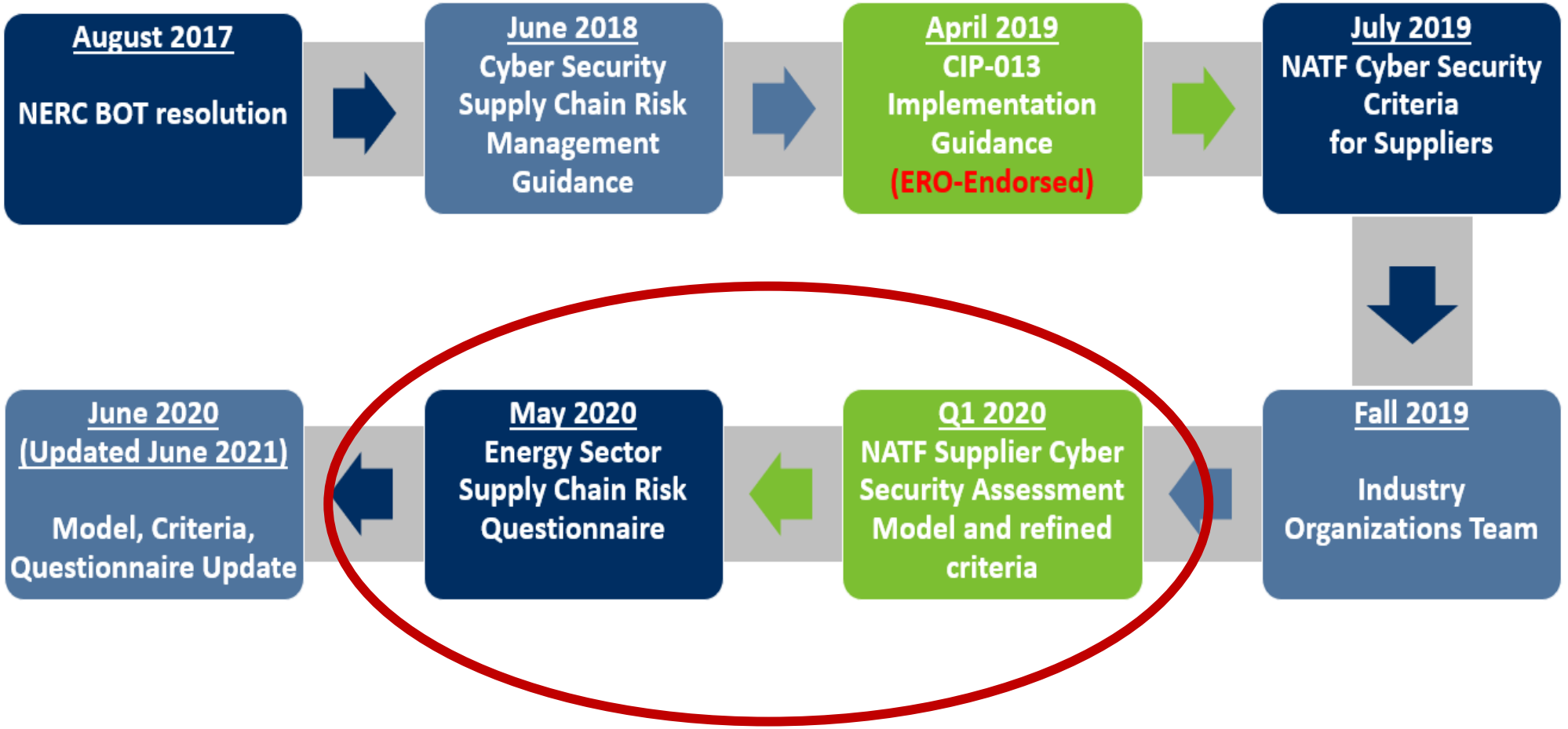
ERO Enterprise endorsed on February 28

- NATF CIP-013 Implementation Guidance – Using Independent Assessments of Vendors
- NATF CIP-013 Implementation Guidance – Supply Chain Risk Management Plans

Providing assurance of alignment between security and compliance

Available on the NERC and NATF public websites

NATF's Supply Chain Journey



Objectives

Security

Identifying and addressing cyber security risks introduced via supply chain

Industry Convergence

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

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)

NATF-led Industry Organizations Team

Organizations, Forums and Working Groups

- AGA
- EC
- EEI
- LPPC
- APPA
- TAPS
- NAGF
- NAESB
- ConEd Working Group
- NERC CCC/RSTC/SCWG
- NRECA

Suppliers

- Hitachi Energy
- GE Grid Software Solutions
- OSI
- Siemens Industry, Inc.
- Schneider Electric
- Schweitzer Engineering
- Dell

Third-Party Assessors

- Ernst & Young
- KPMG LLP
- PWC
- Deloitte

Organizations providing support products or services

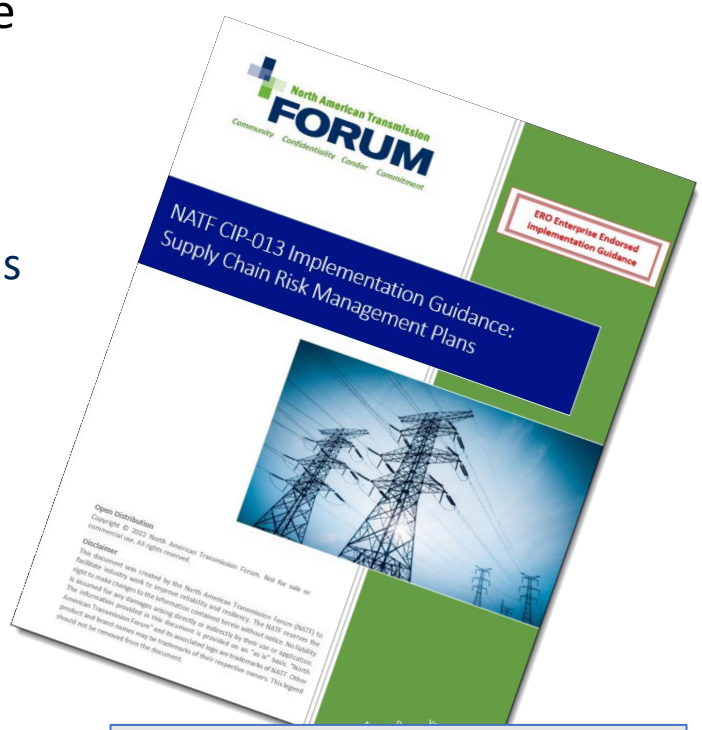
- EPRI
- Fortress/A2V
- KY3P
- UL

Today's Overview

Implementation Guidance	Processes	Tools
• NATF CIP-013 Implementation Guidance – Using Independent Assessments of Vendors • NATF CIP-013 Implementation Guidance – Supply Chain Risk Management Plans	• NATF Supply Chain Security Assessment Model (Model) • NATF Criteria and Questionnaire Revision Process (Revision Process)	• NATF Supply Chain Security Criteria (NATF Criteria) • Energy Sector Supply Chain Risk Questionnaire (Questionnaire) • Additional Tools from industry partners

Using Independent Assessments of Vendors

- Updates previously endorsed NATF implementation guidance to include CIP-013-2 and incorporates, by reference into the implementation guidance, the criteria, questionnaire, and associated revision process.
- Responsible Entity's Supply Chain Risk Management Plan includes:
  - process for assessing risk in procuring and installing CIP-013 Applicable Systems and transitioning from one vendor to another vendor.
  - Process to incorporate rely on independent assessments of vendors
    - Obtain an independent third-party assessment from an auditor or assessor
    - Determine auditor or assessor's qualifications
    - Evaluate scope and results of the third-party's assessment
      - Does the scope cover what is needed for the risk of the procurement
      - At a minimum, does it cover the CIP-013 requirement R1, part 1.2
    - Determine what existing or additional mitigating actions are appropriate to manage risk



Providing assurance of alignment between security and compliance

Supply Chain Risk Management Plans

- Uses the NATF Supply Chain Security Assessment Model to develop a supply chain cyber security risk management plan(s)
- **Focus is on security**
- **Incorporates the NATF Criteria and Questionnaire**
- Encompasses the compliance requirements for planning for the procurement of CIP-013 Applicable Systems to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from
  - procuring and installing vendor equipment and software, and
  - transitions from one vendor(s) to another vendor(s)
- Addresses the six risk areas identified in Requirement R1, Part 1.2

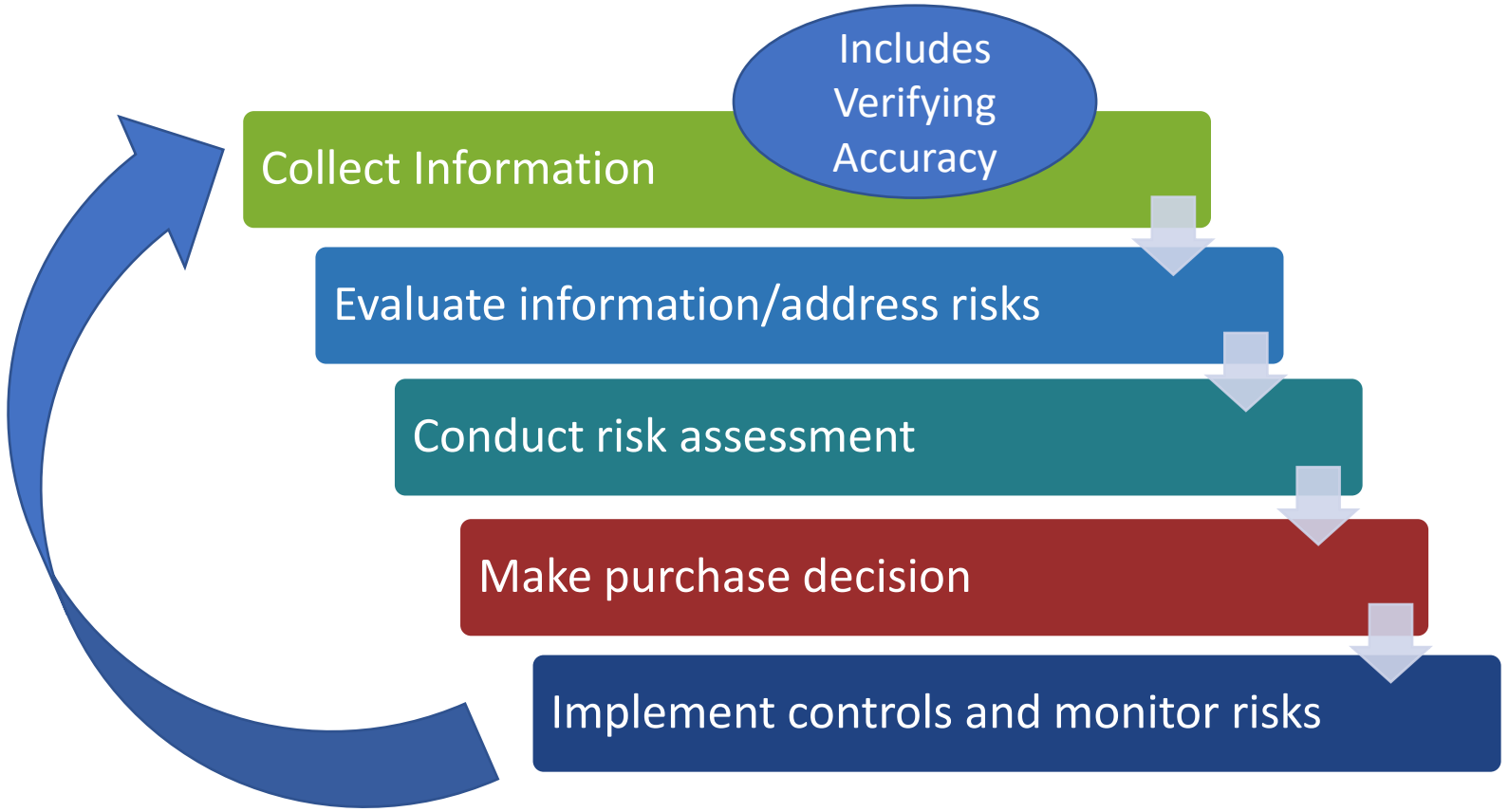
Providing assurance of alignment between security and compliance

North American Transmission FORUM

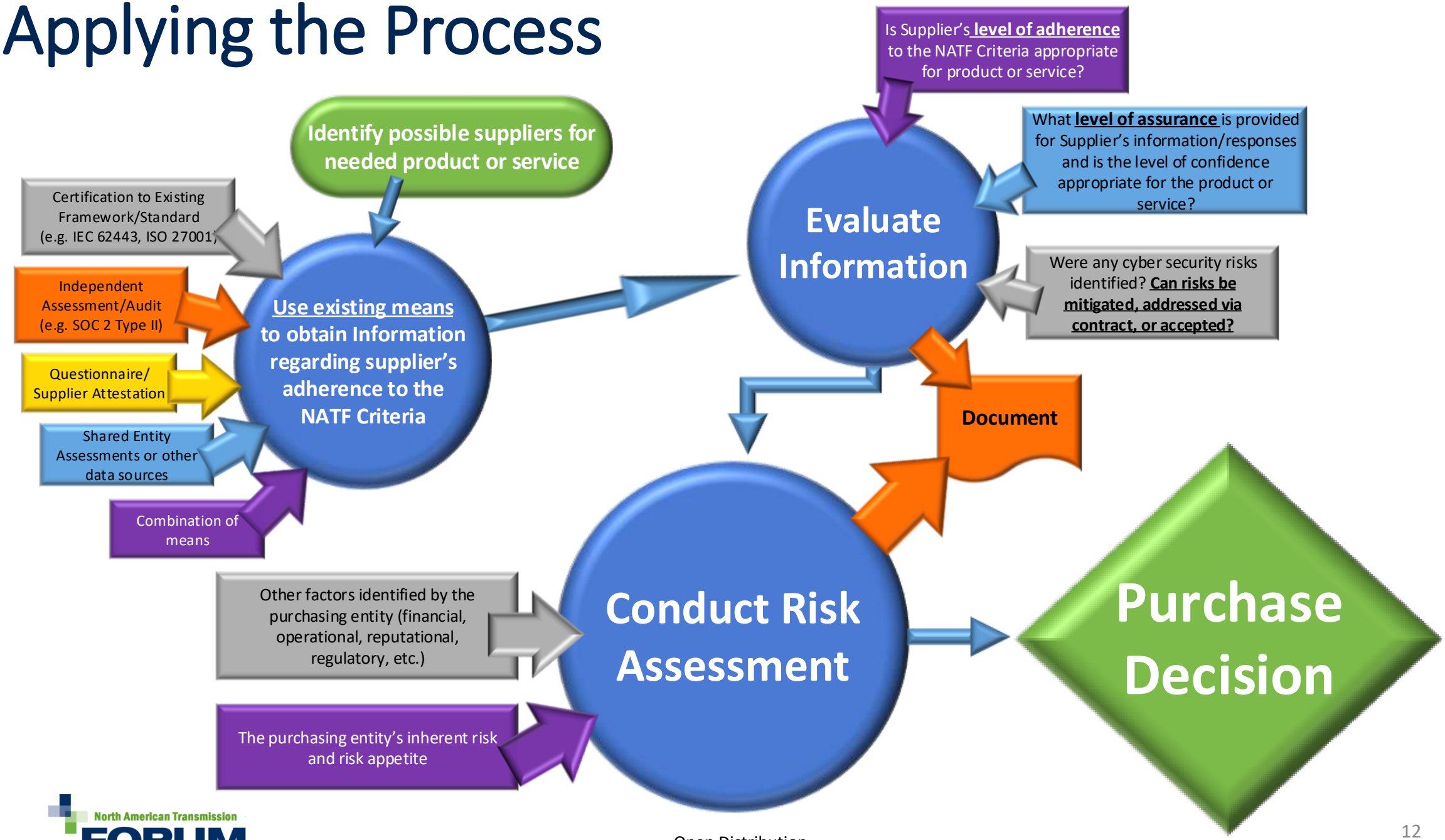
The NATF Supply Chain Security Assessment Model - Applying the Process

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

Supply Chain Security Assessment Model



Applying the Process



Collect Information and Verify

Collect Information

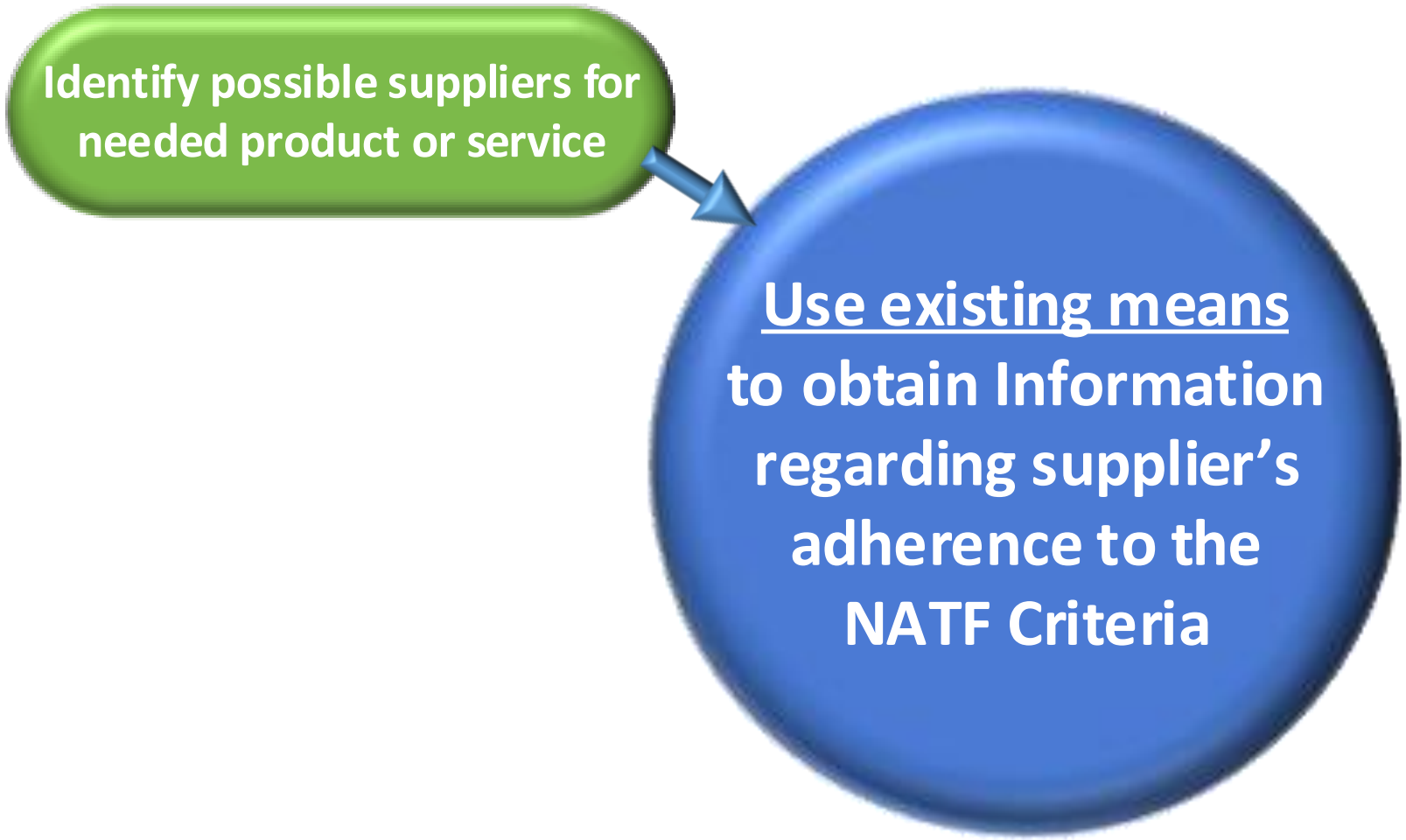
- Collect it from Suppliers yourself
  - NATF Criteria
  - Questionnaire
- Use a solution-provider service
- Obtain a “shared audit” from another entity

Verify - Obtain Assurance of Accuracy

- Third-party Assessments
  - Obtain a qualified assessors’ third-party assessment, certification and/or independent audit that addresses NATF Criteria and Questionnaire
- Obtain a validation/verification from a solution provider
  - Solution-provider risk assessments
  - Shared assessments
- Conduct your own validation/verification
  - Obtain evidence from supplier to conduct your own validation/verification

Collect Information

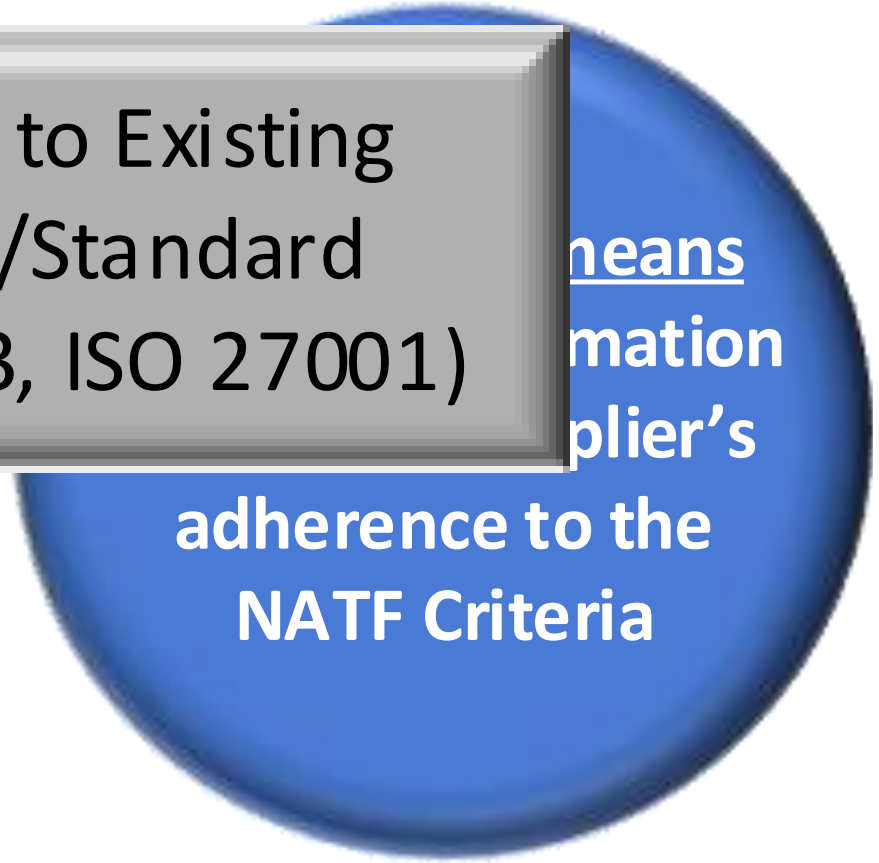
Obtain Information on Supplier's Adherence



Collect Information

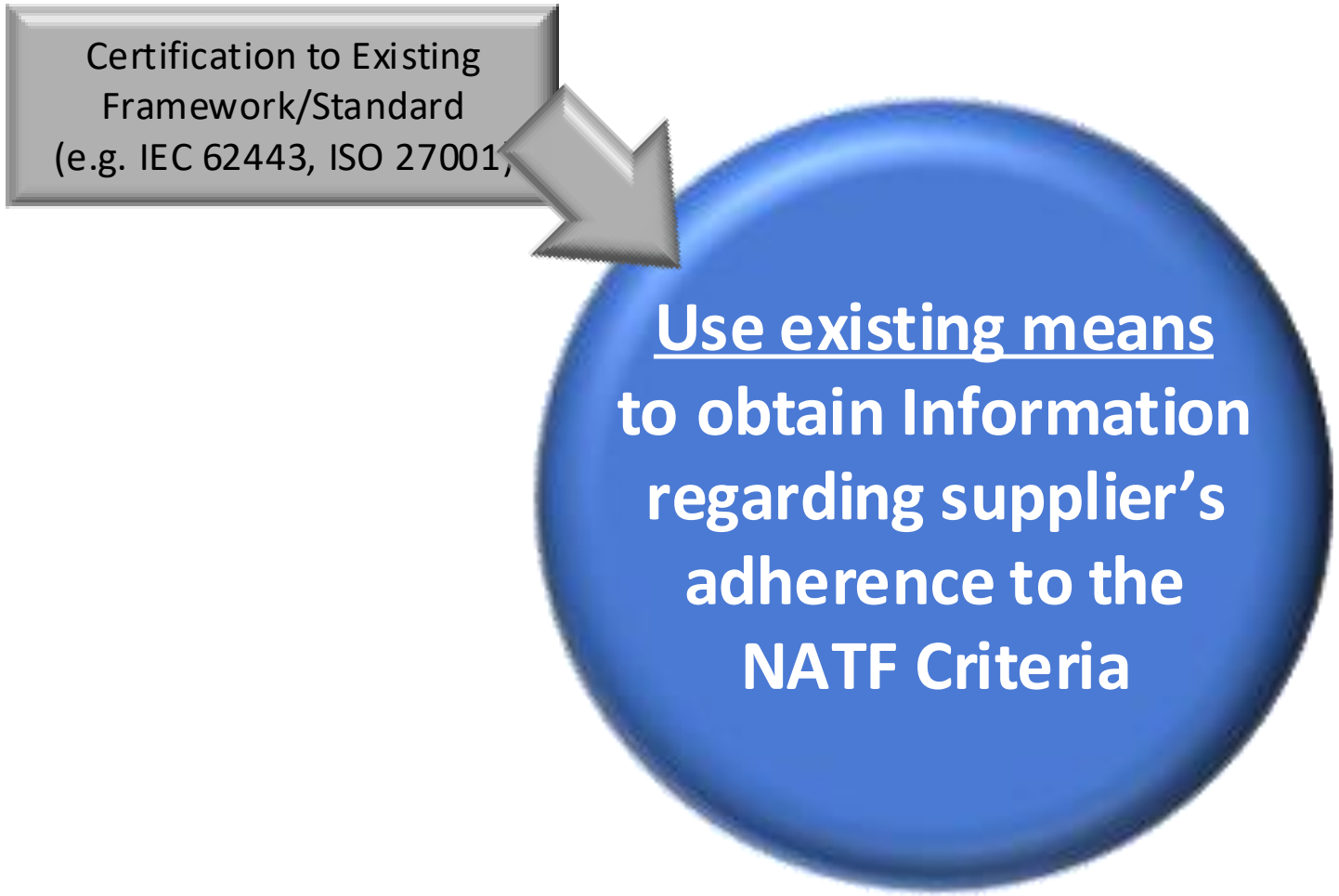
Obtain Information on Supplier's Adherence

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



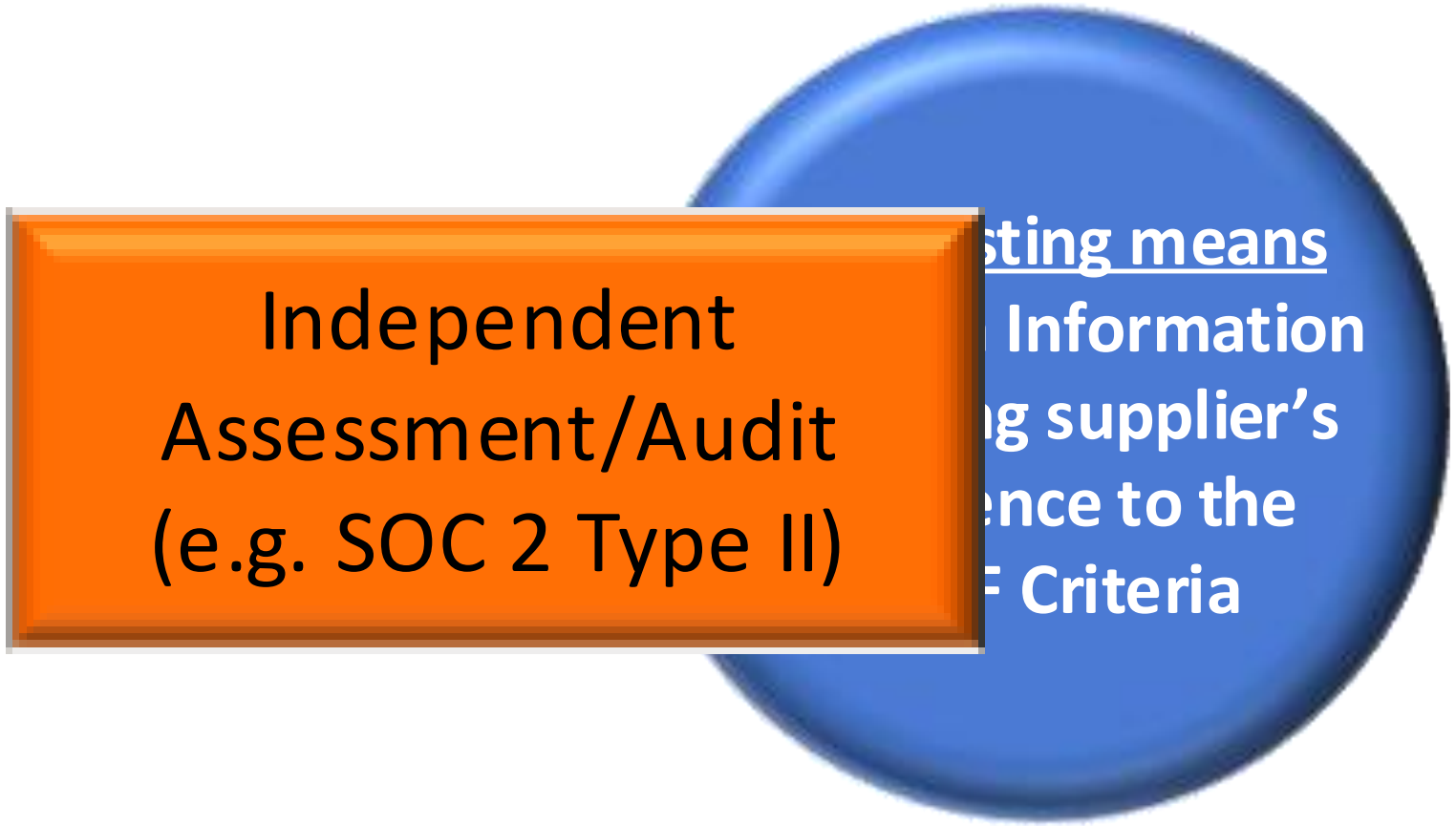
Collect Information

Obtain Information on Supplier's Adherence



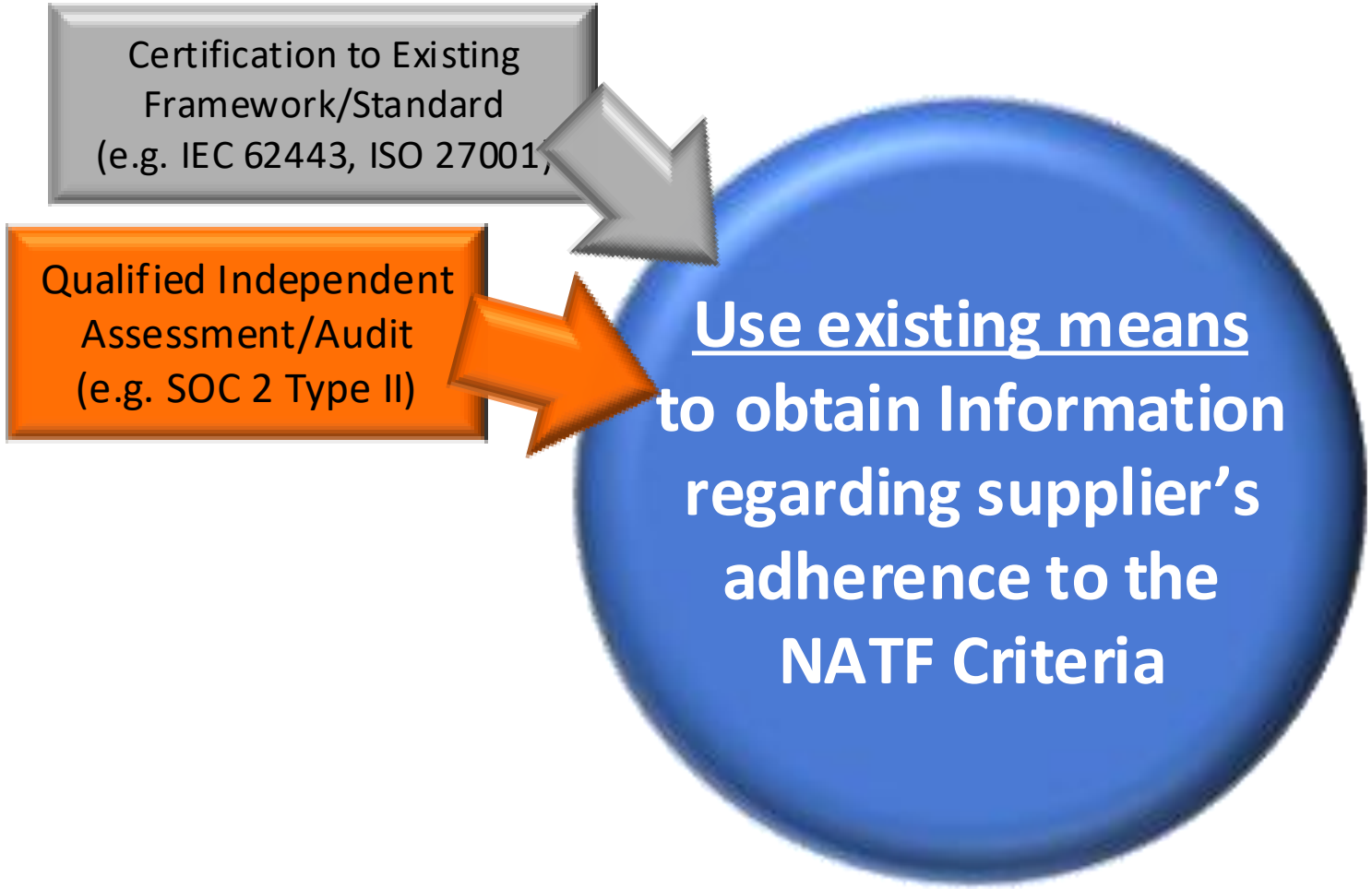
Collect Information

Obtain Information on Supplier's Adherence



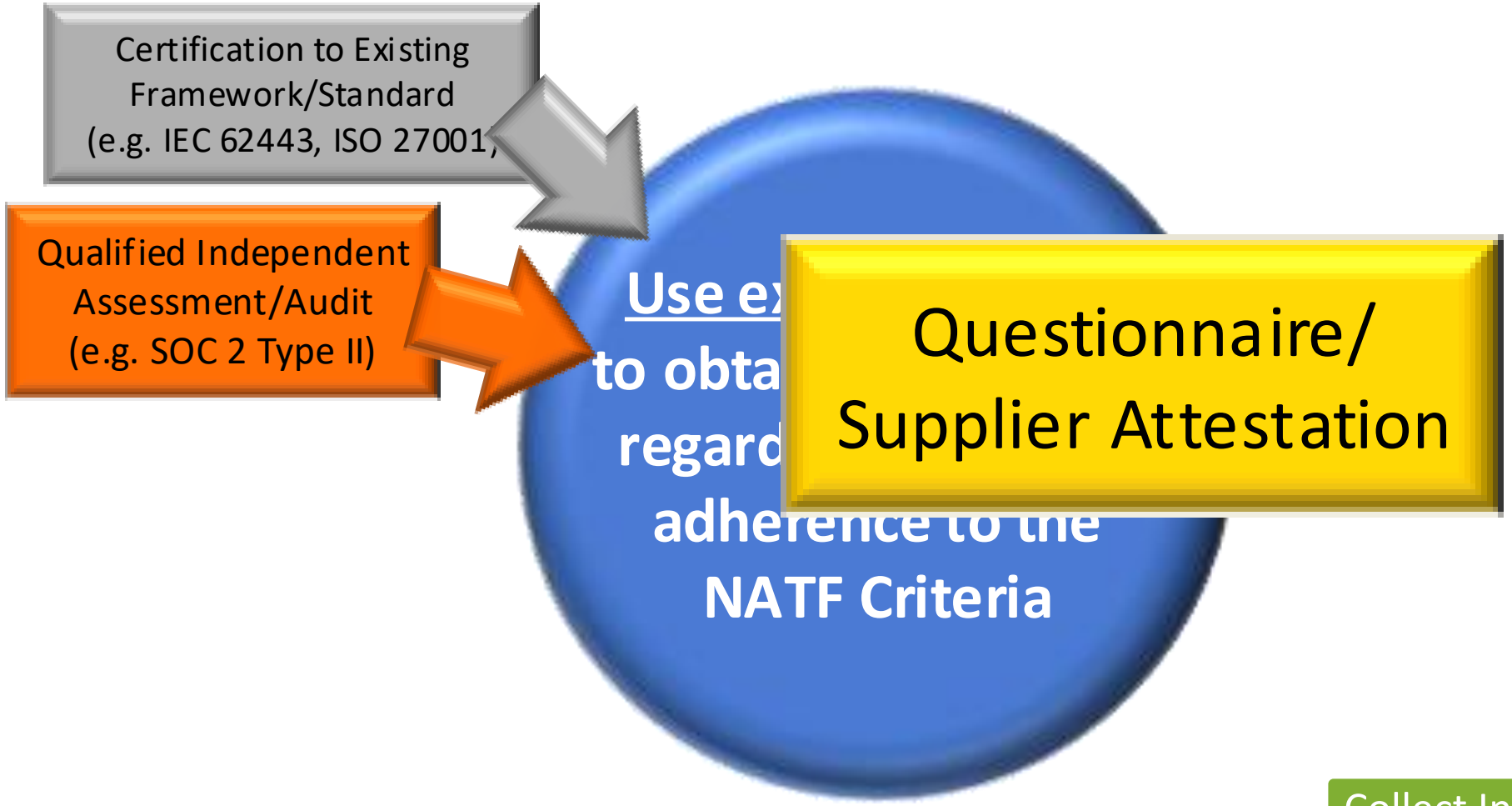
Collect Information

Obtain Information on Supplier's Adherence



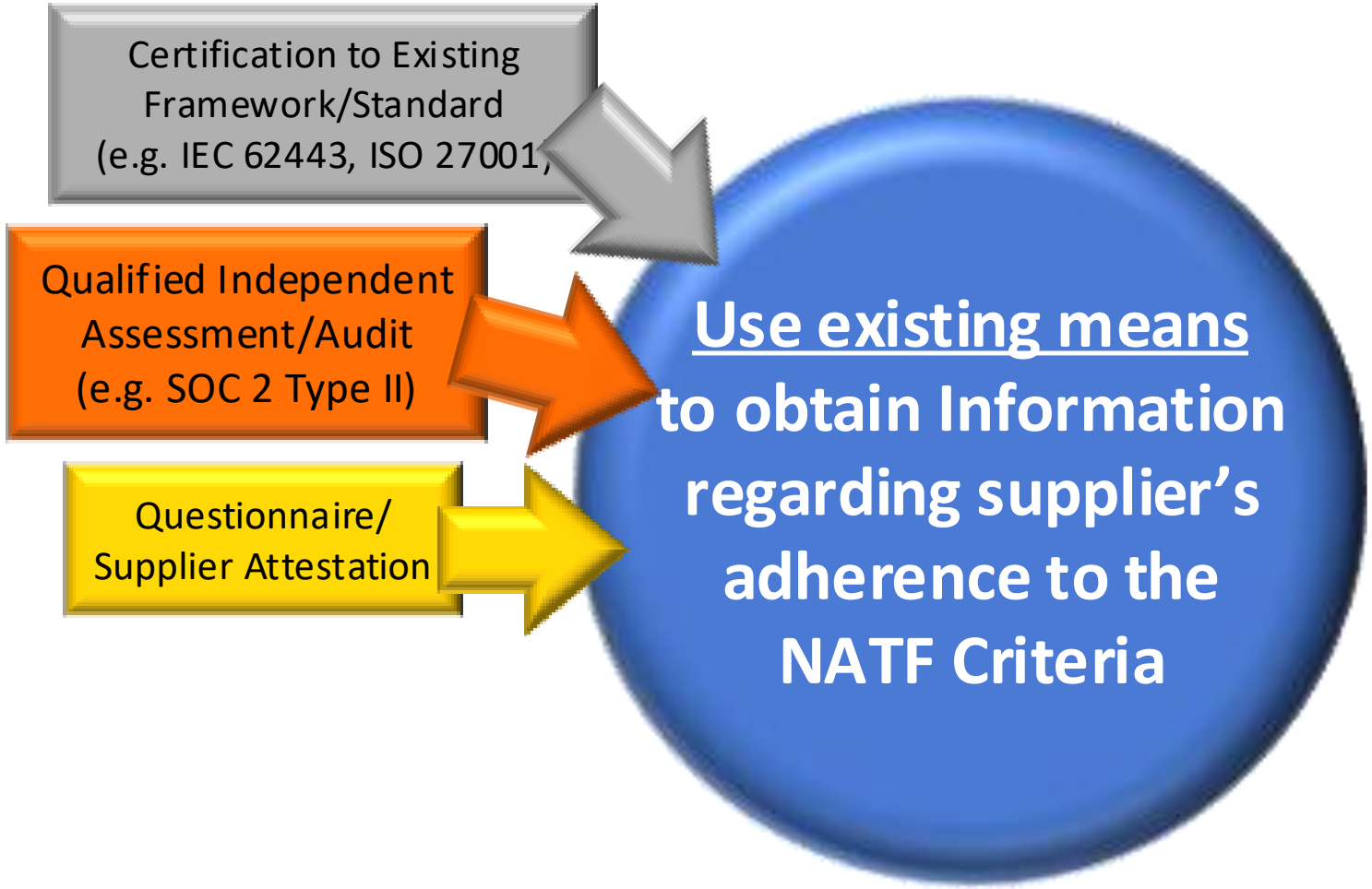
Collect Information

Obtain Information on Supplier's Adherence



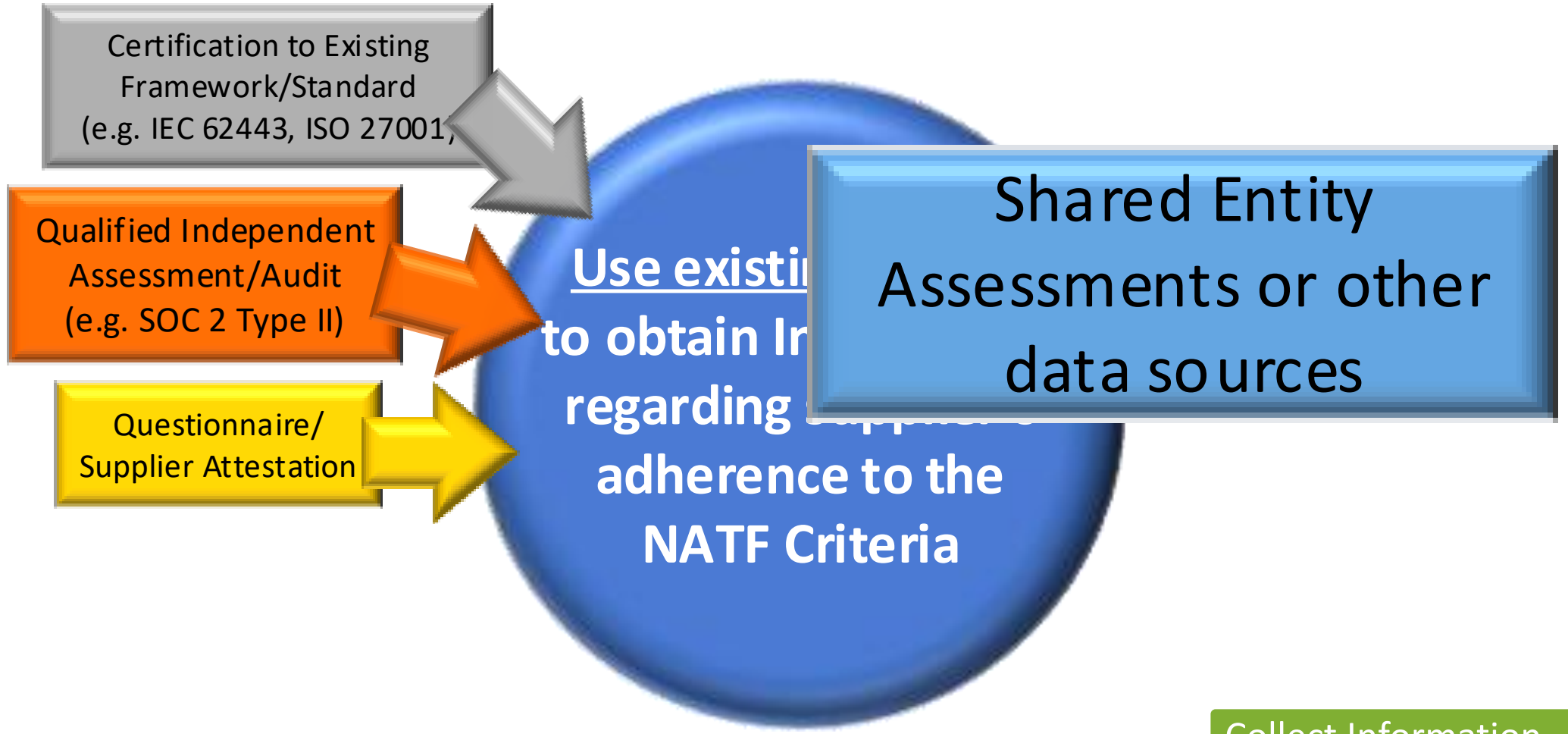
Collect Information

Obtain Information on Supplier's Adherence



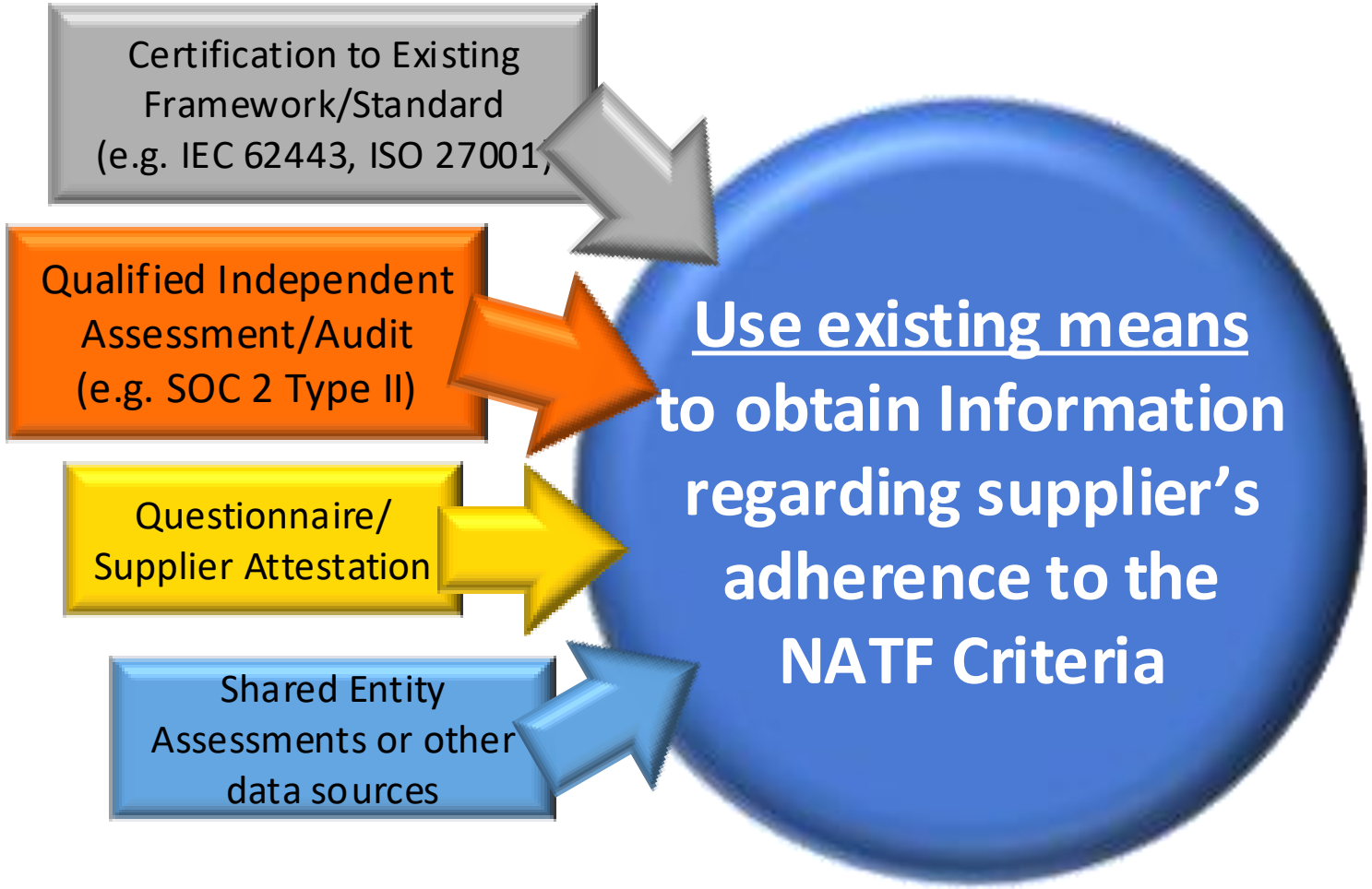
Collect Information

Obtain Information on Supplier's Adherence



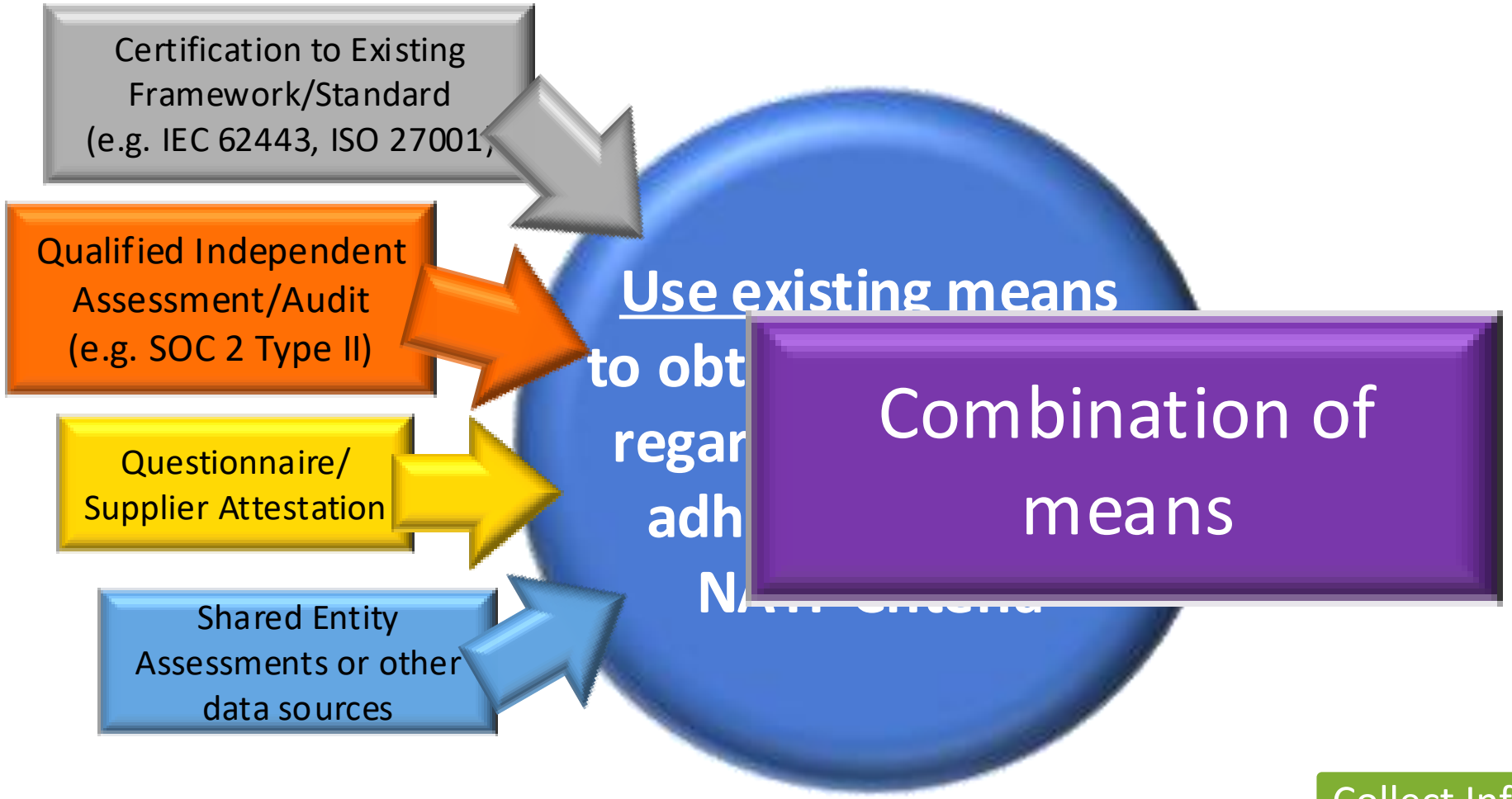
Collect Information

Obtain Information on Supplier's Adherence



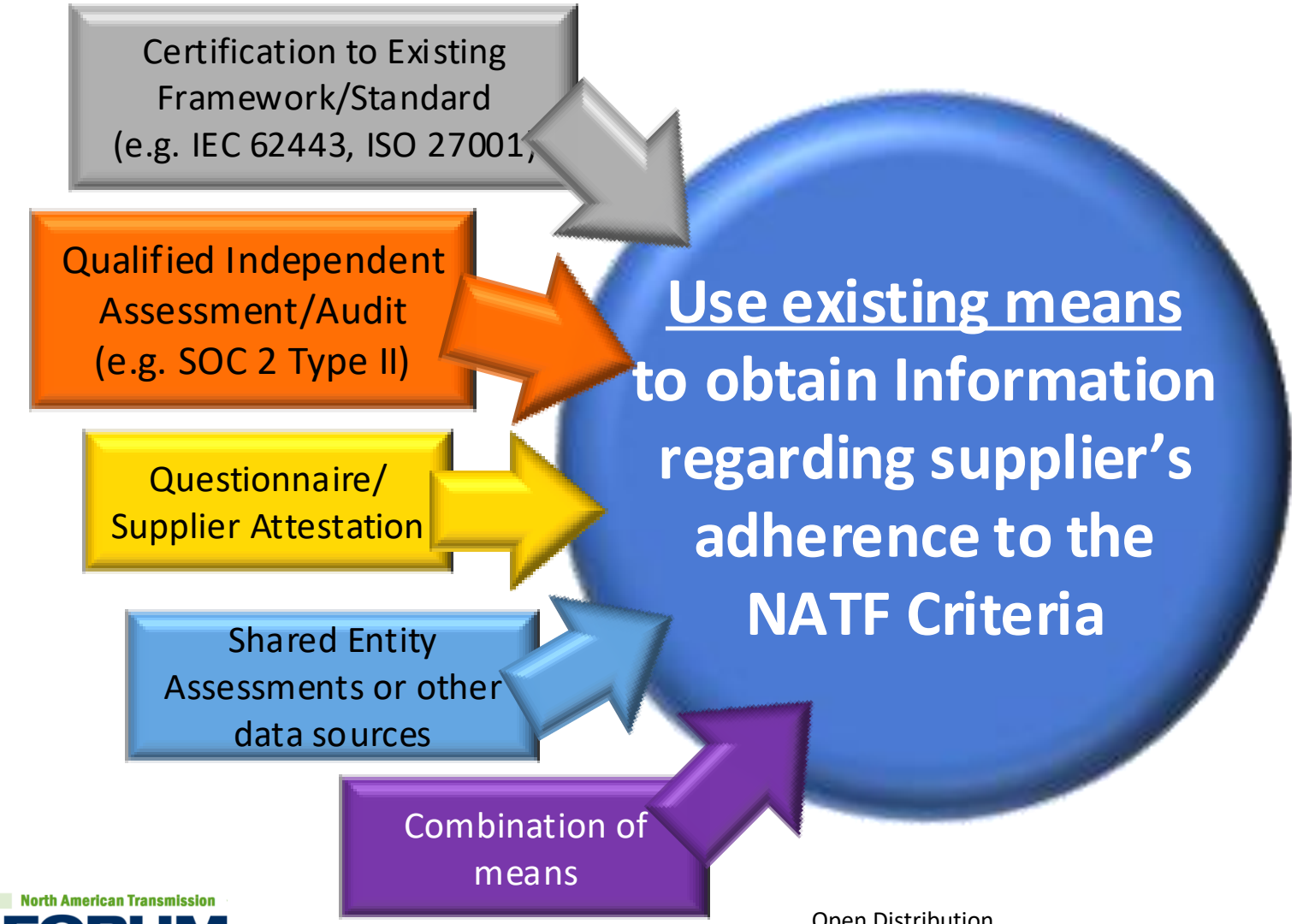
Collect Information

Obtain Information on Supplier's Adherence



Collect Information

Obtain Information on Supplier's Adherence



Collect Information

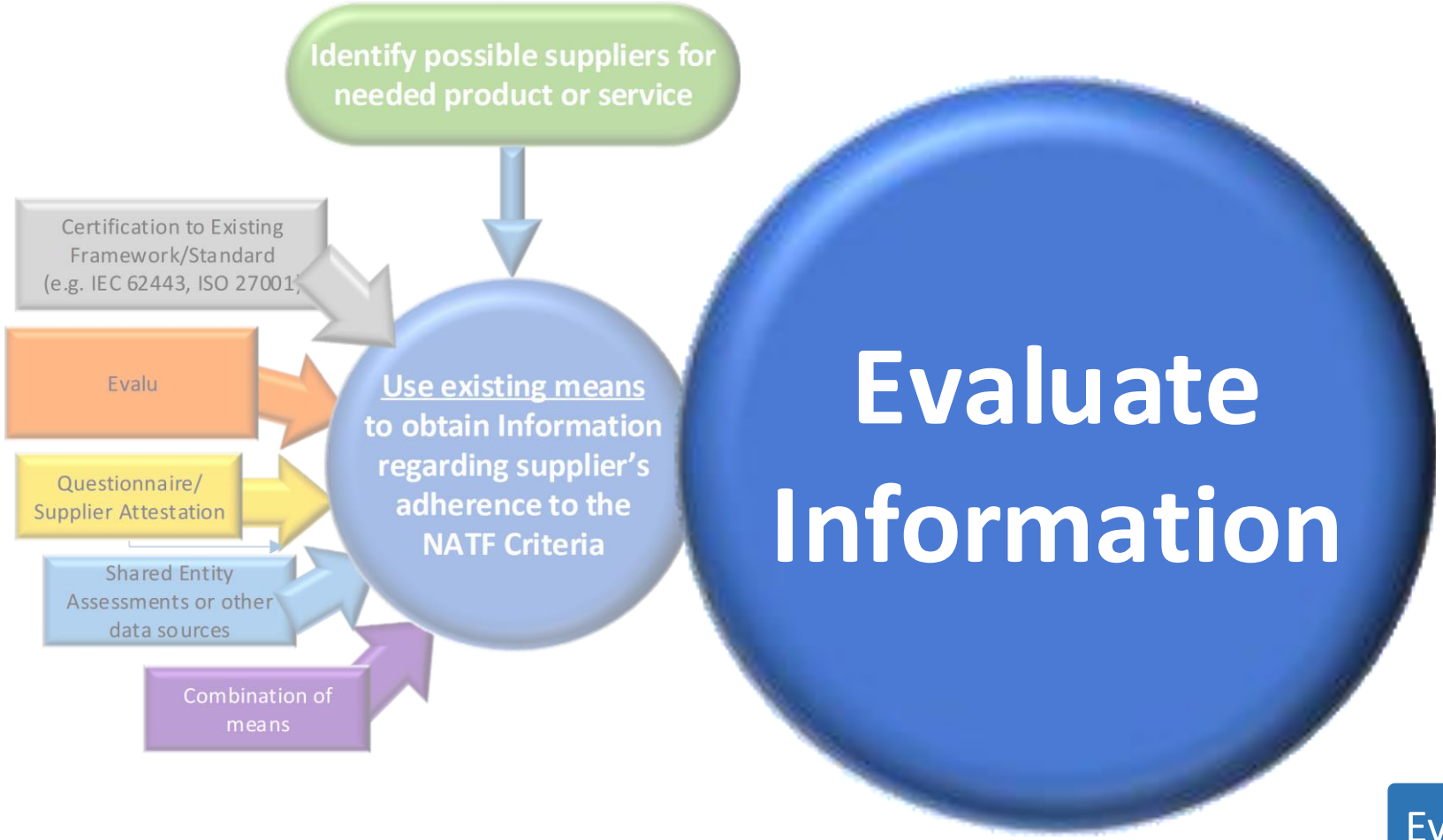
Evaluate Information/Address Risks

- Evaluate the information collected
  - The level of the supplier's adherence to the NATF Criteria and/or response to the Questionnaire
  - The level of assurance the supplier has provided for its responses

- Determine whether identified risks could be mitigated or accepted
  - Mitigated by the supplier
  - Mitigated by your organization

Evaluate information/ address risks

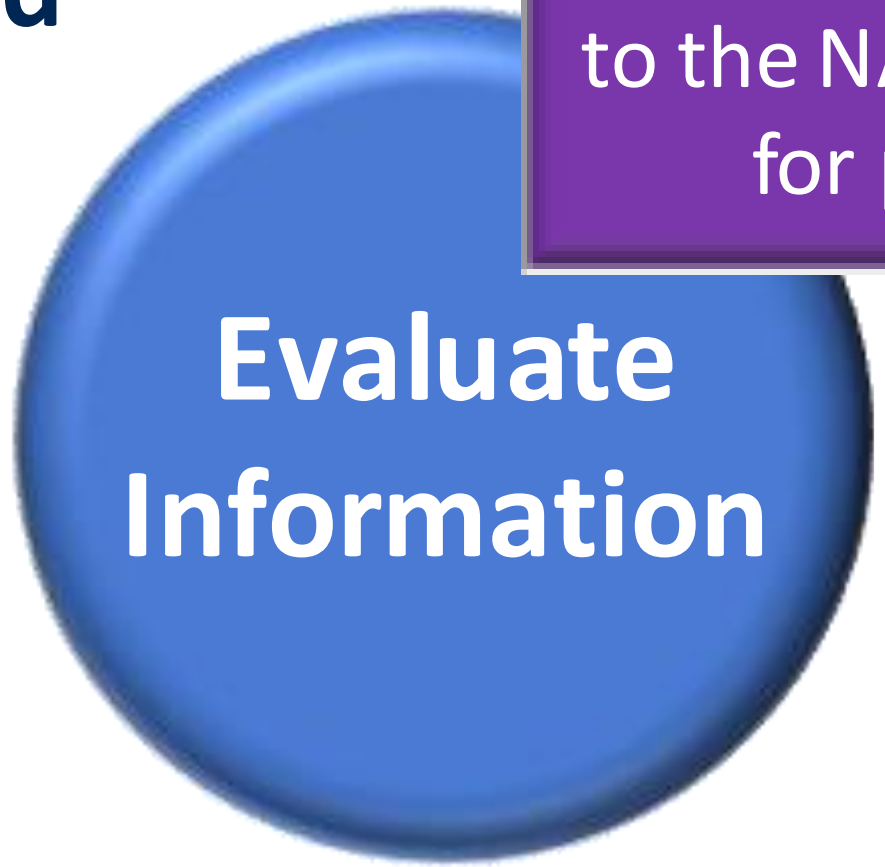
Evaluate the Information Obtained



Evaluate information/ address risks

Evaluate the Information Obtained

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



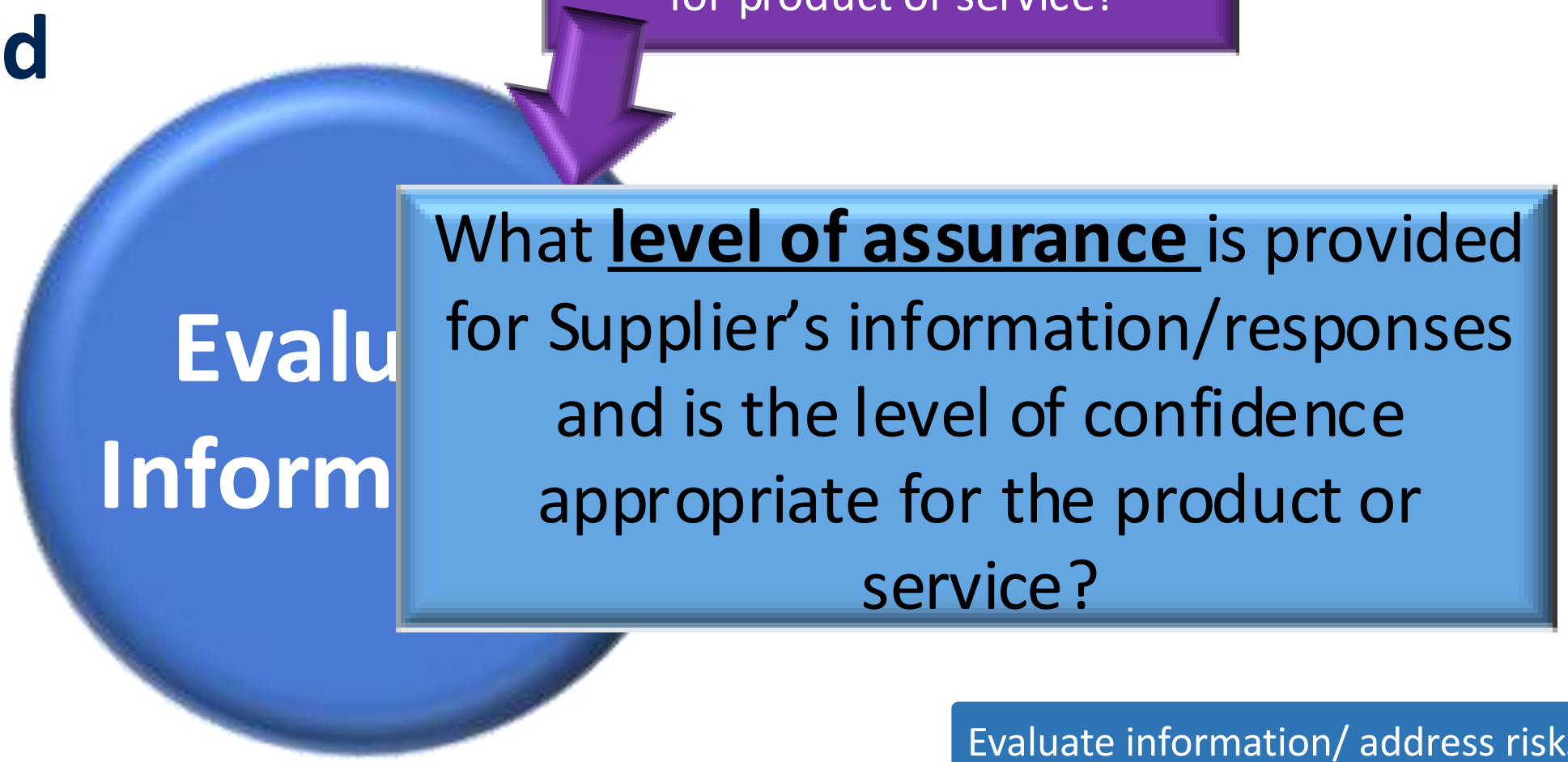
Evaluate information/ address risks

Evaluate the Information Obtained

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

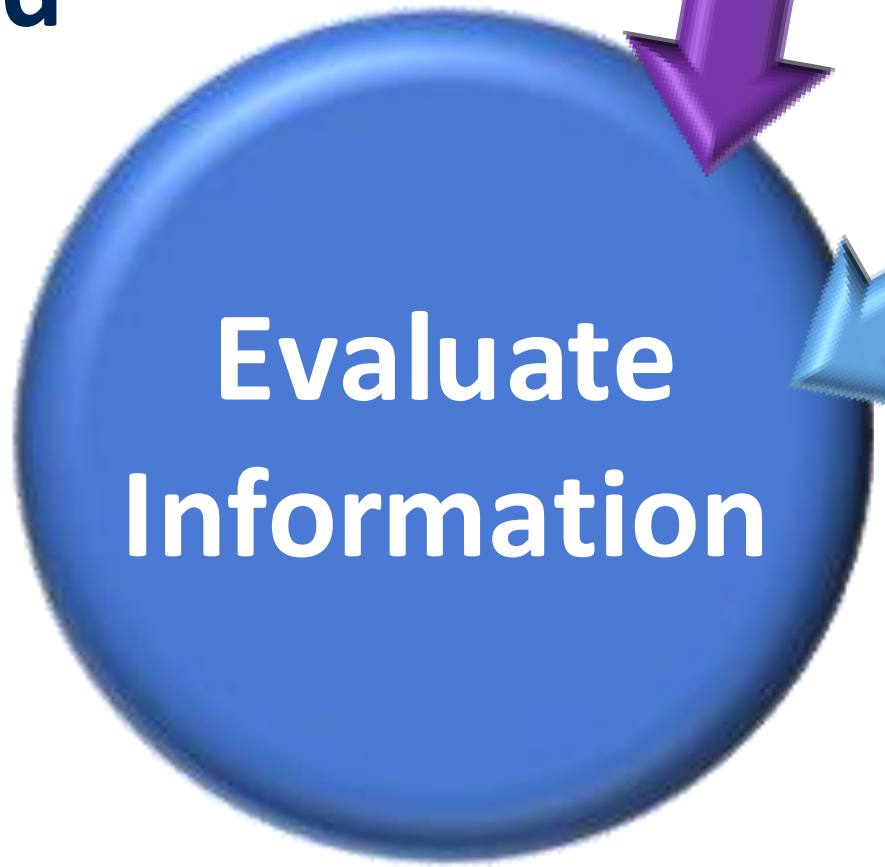
Evaluate information/ address risks

Evaluate the Information Obtained



Evaluate information/ address risks

Evaluate the Information Obtained

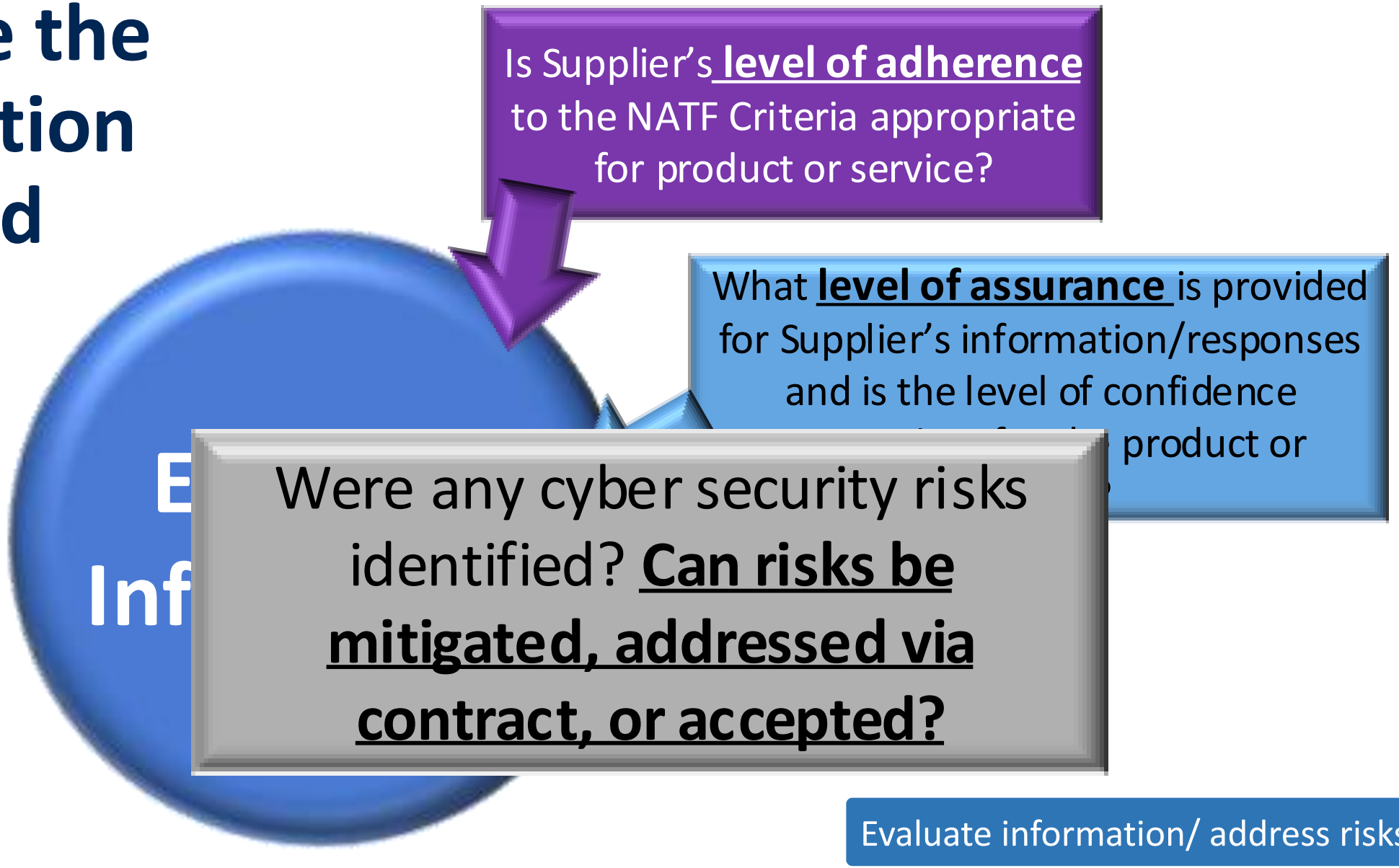


Is Supplier's **level of adherence** to the NATF Criteria appropriate for product or service?

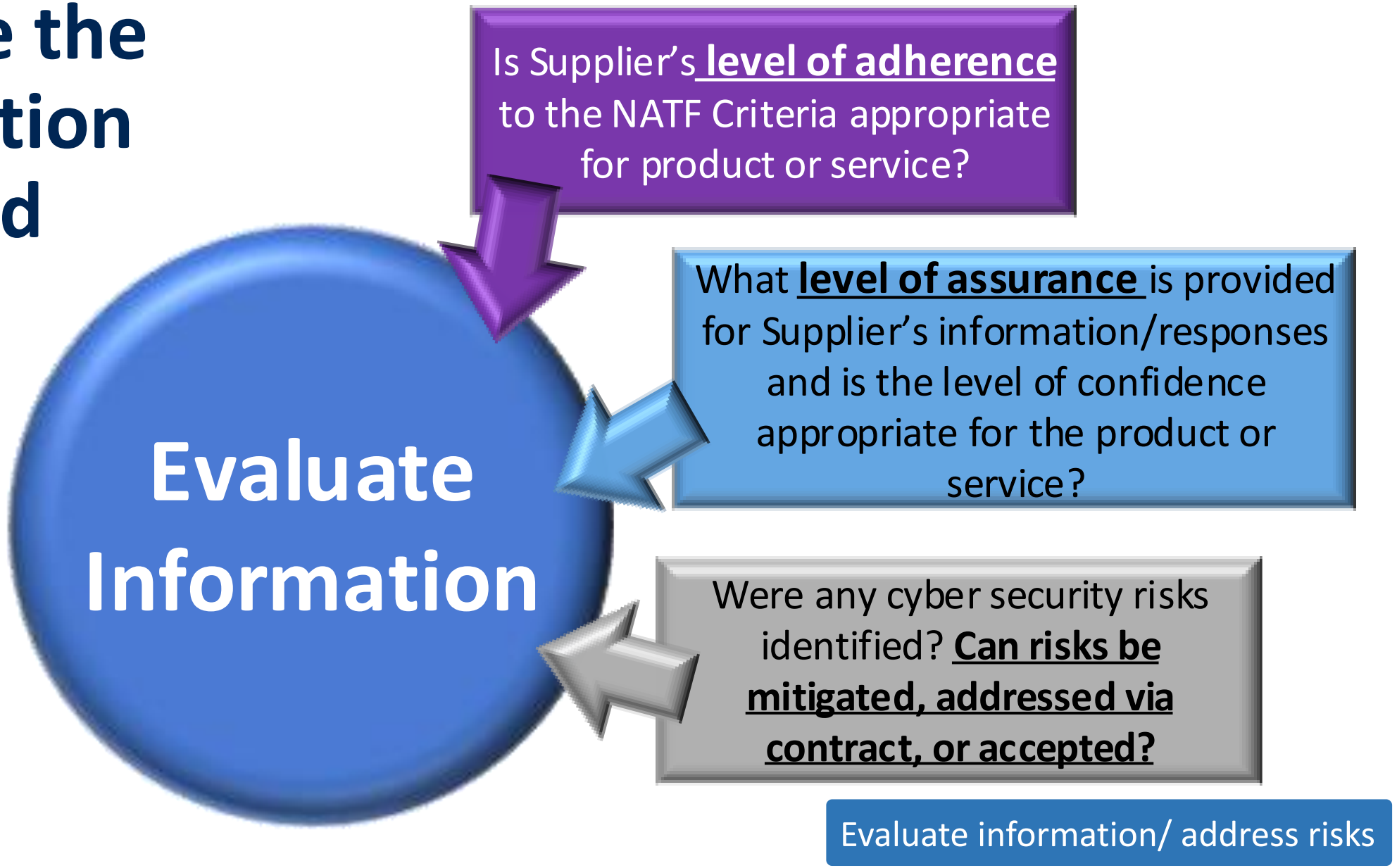
What **level of assurance** is provided for Supplier's information/responses and is the level of confidence appropriate for the product or service?

Evaluate information/ address risks

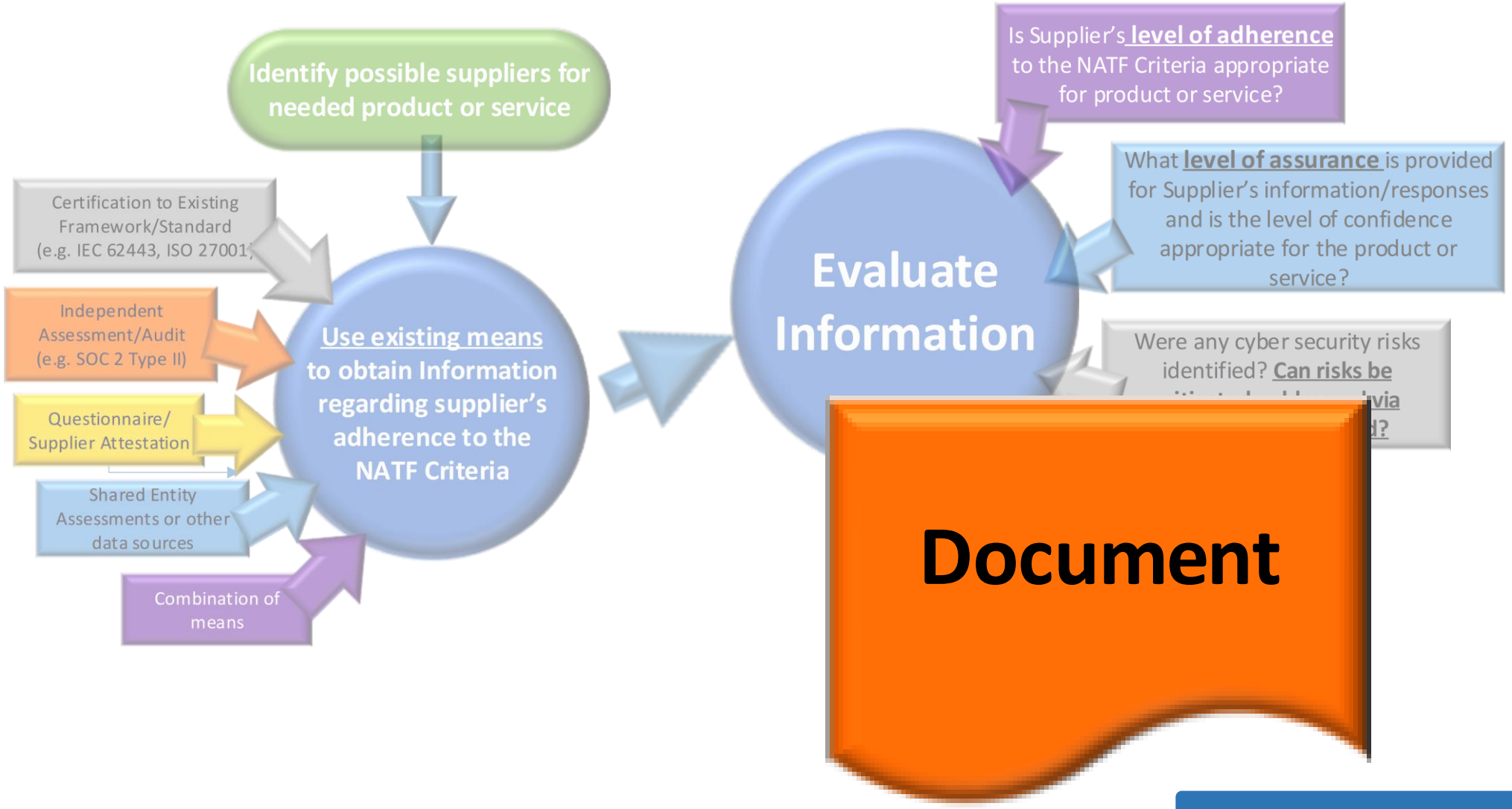
Evaluate the Information Obtained



Evaluate the Information Obtained



Document!



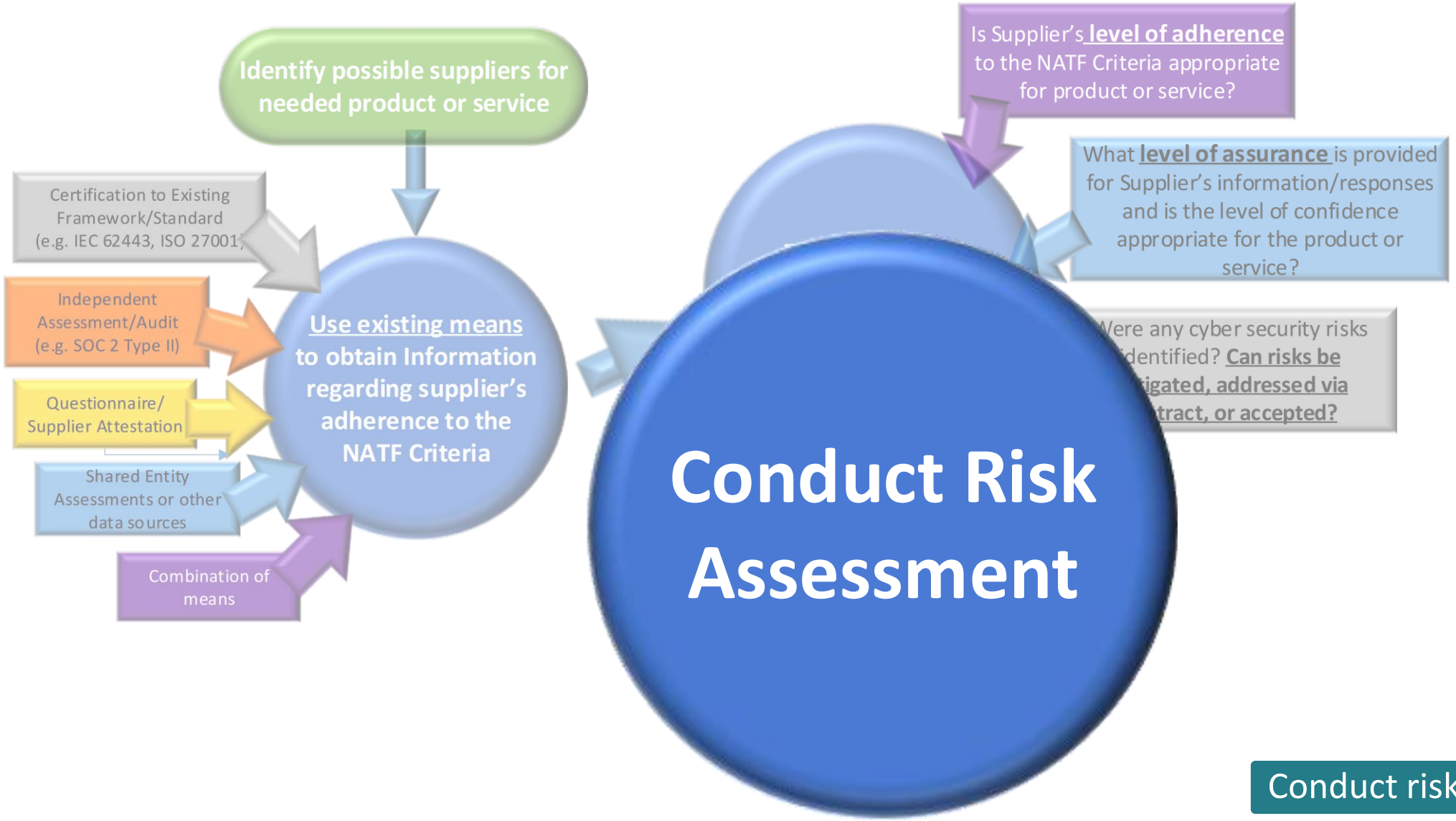
Evaluate information/ address risks

Conduct Risk Assessment

- Have a methodology to conduct a supplier risk assessment
  - Based on requirements and residual risks, conduct a risk assessment to determine which suppliers could provide the product or service
  - The Model does not prescribe how to conduct the risk assessment
- Document the results of your supplier risk assessment

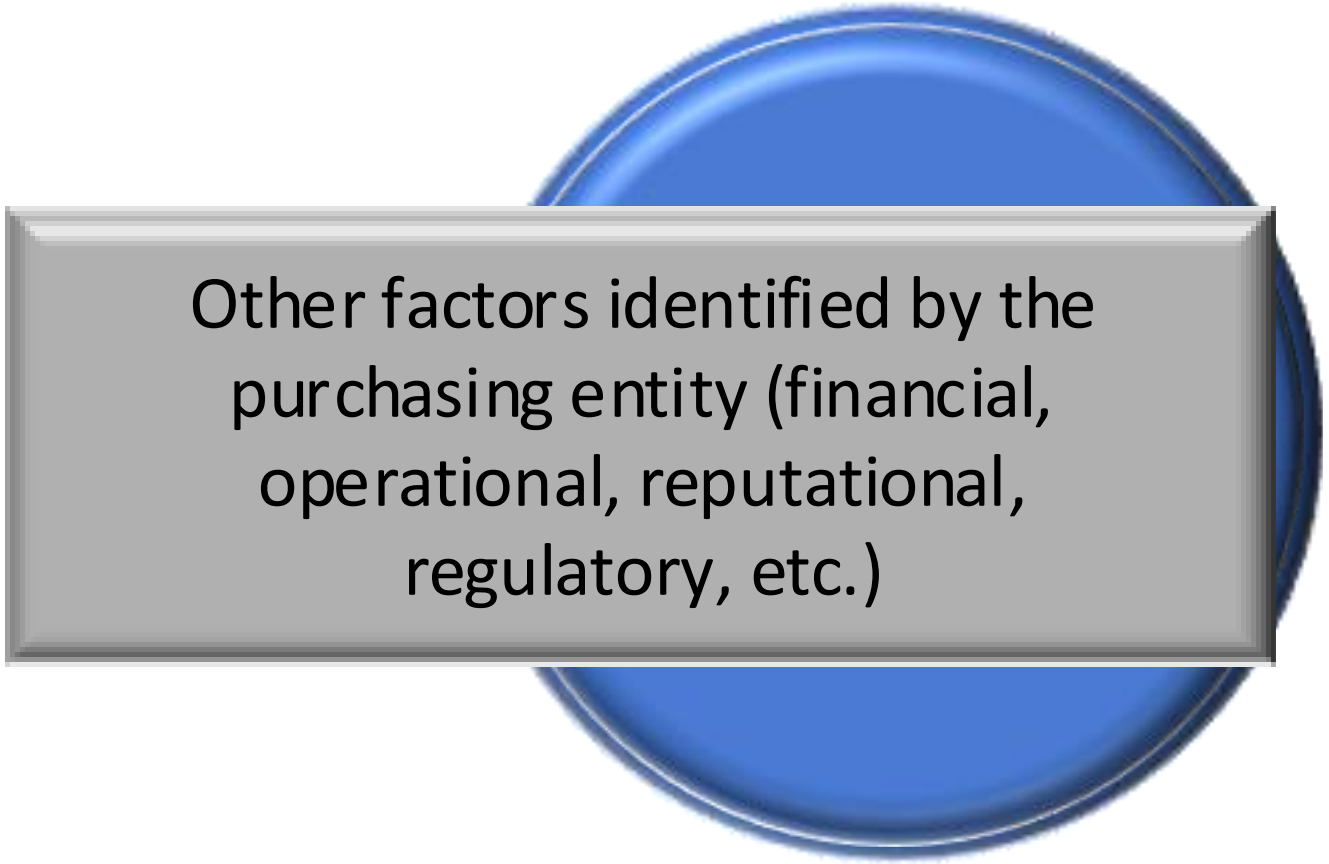
Conduct risk assessment

Conduct Risk Assessment



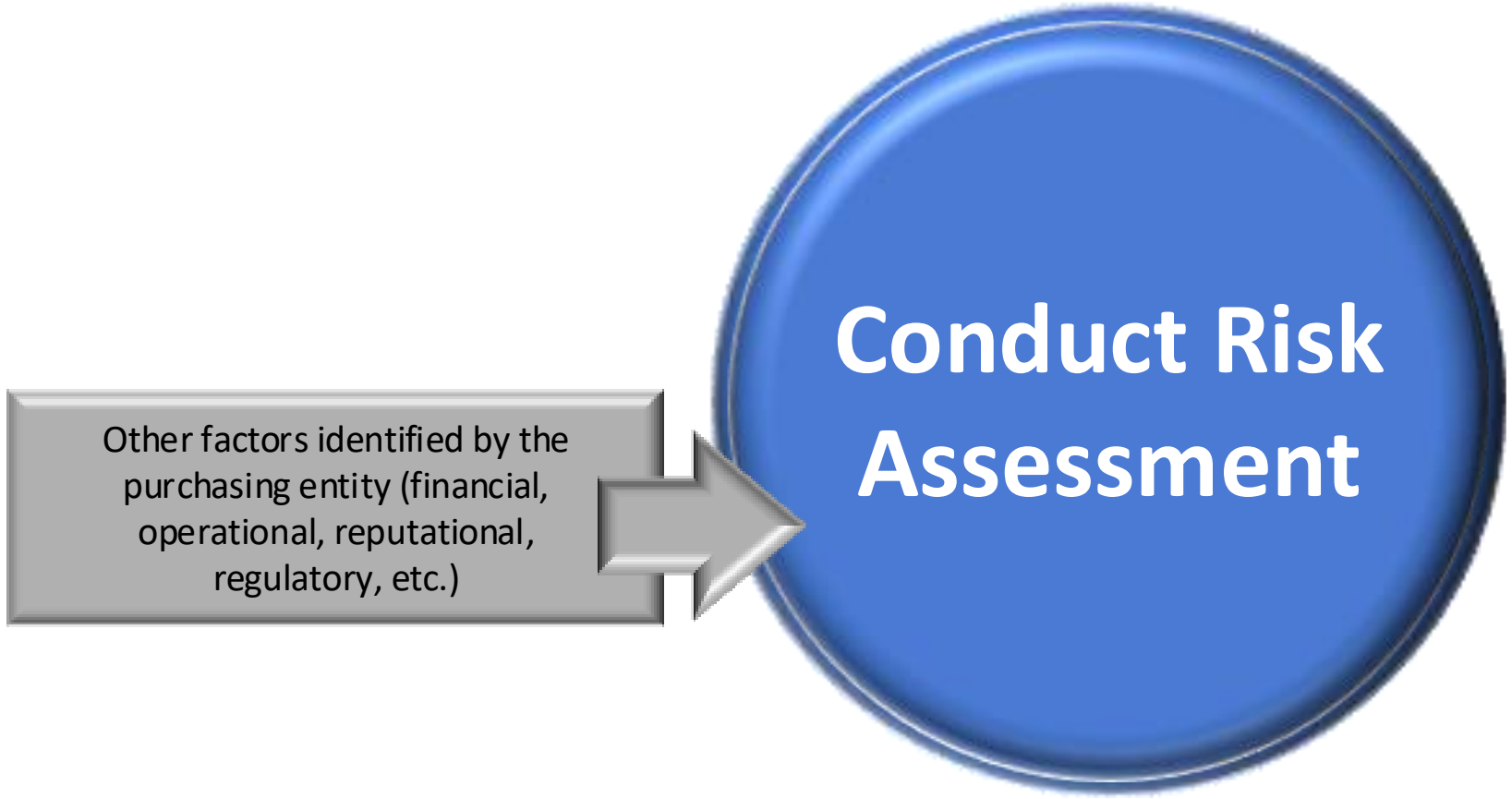
Conduct risk assessment

Conduct Risk Assessment



Conduct risk assessment

Conduct Risk Assessment

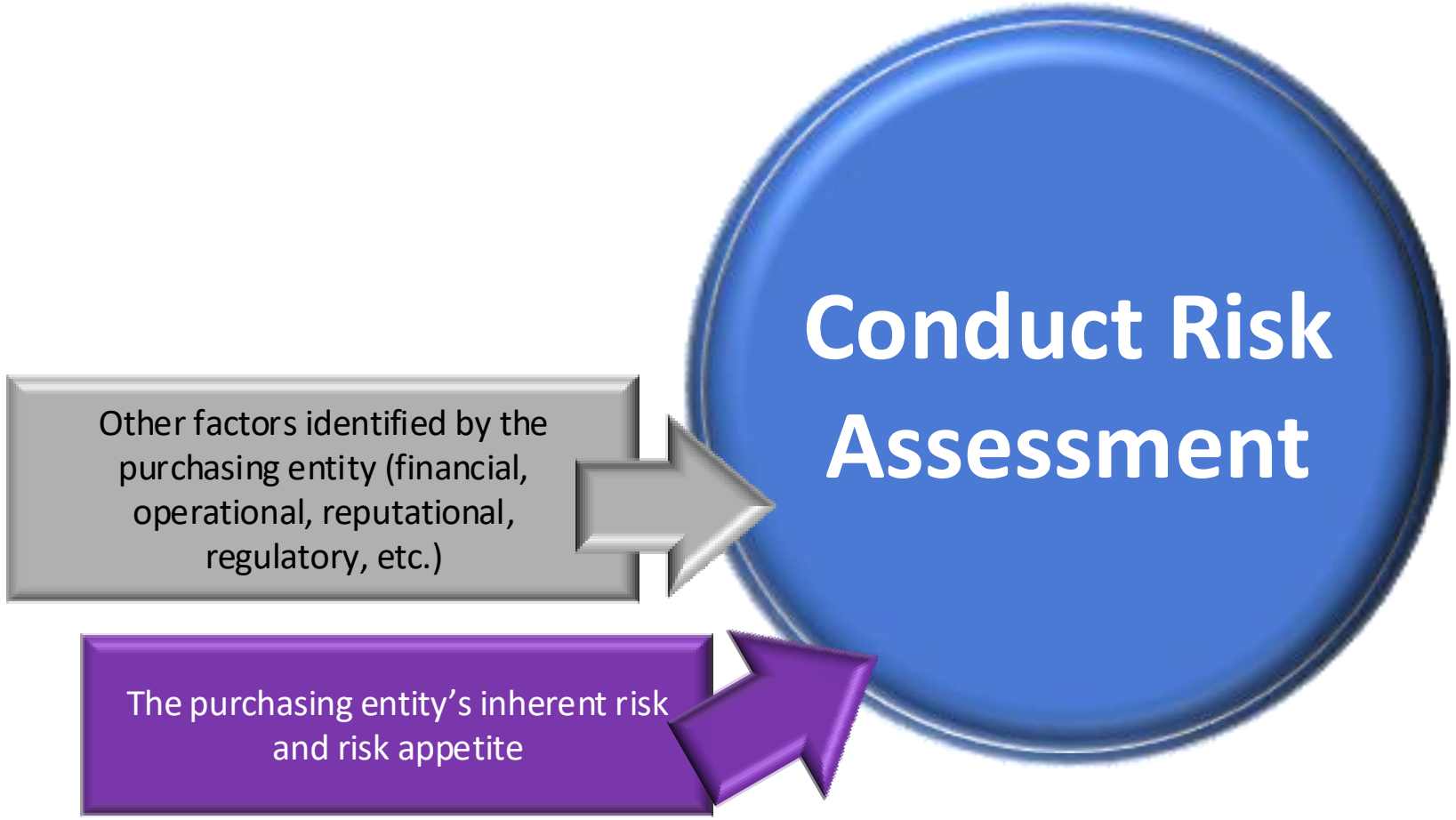


Conduct risk assessment

Conduct Risk Assessment

Conduct risk assessment

Conduct Risk Assessment



Conduct risk assessment

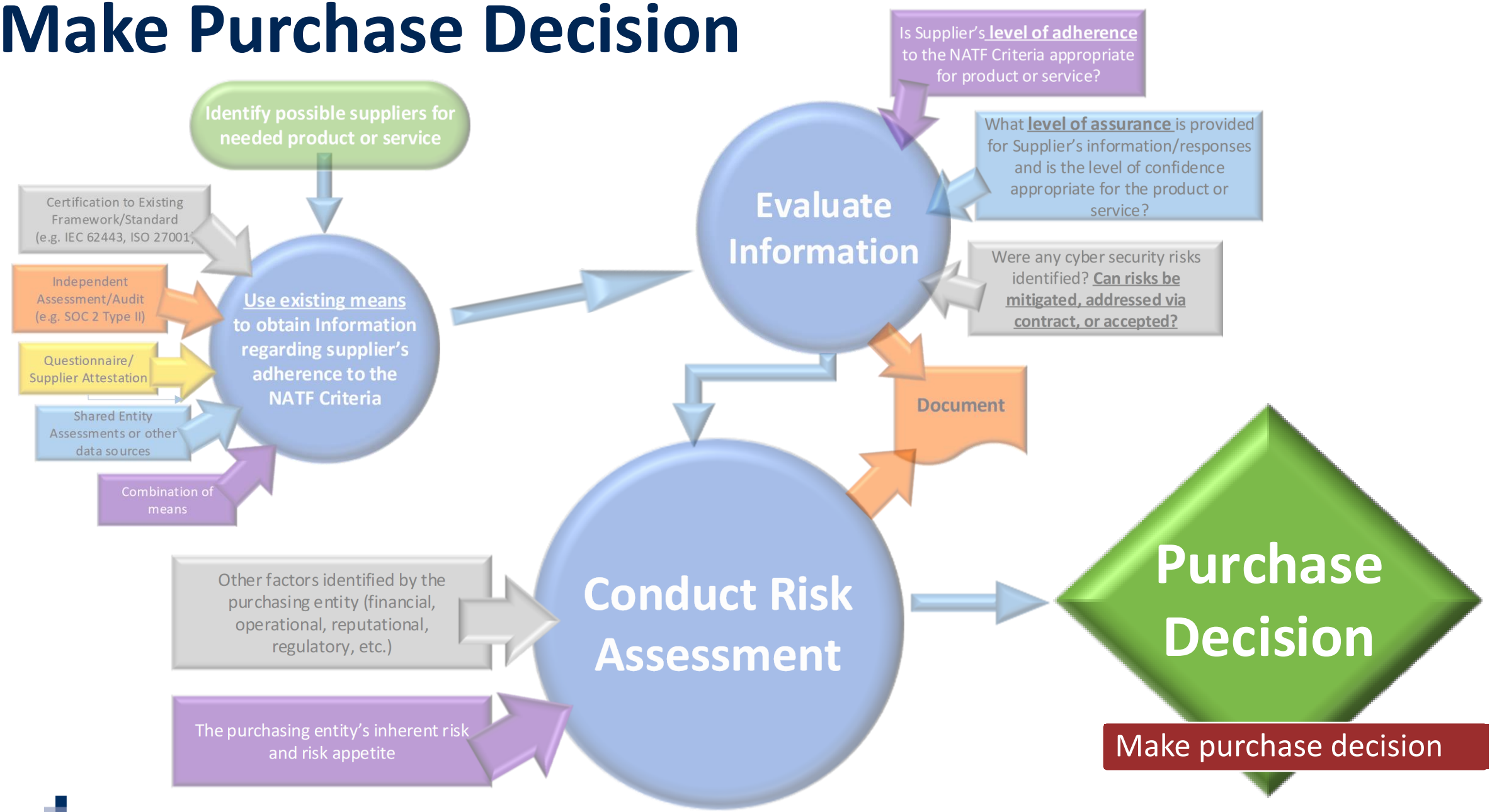
Make Purchase Decision

- Develop a cross-functional process to select supplier, considering:
  - Information from the supplier risk assessment
  - Entity risk tolerance
  - Other entity-identified factors (e.g., financial, supplier support levels, supplier reputation)

- Determine whether mitigation for identified risks can be included in contracts

Make purchase decision

Make Purchase Decision

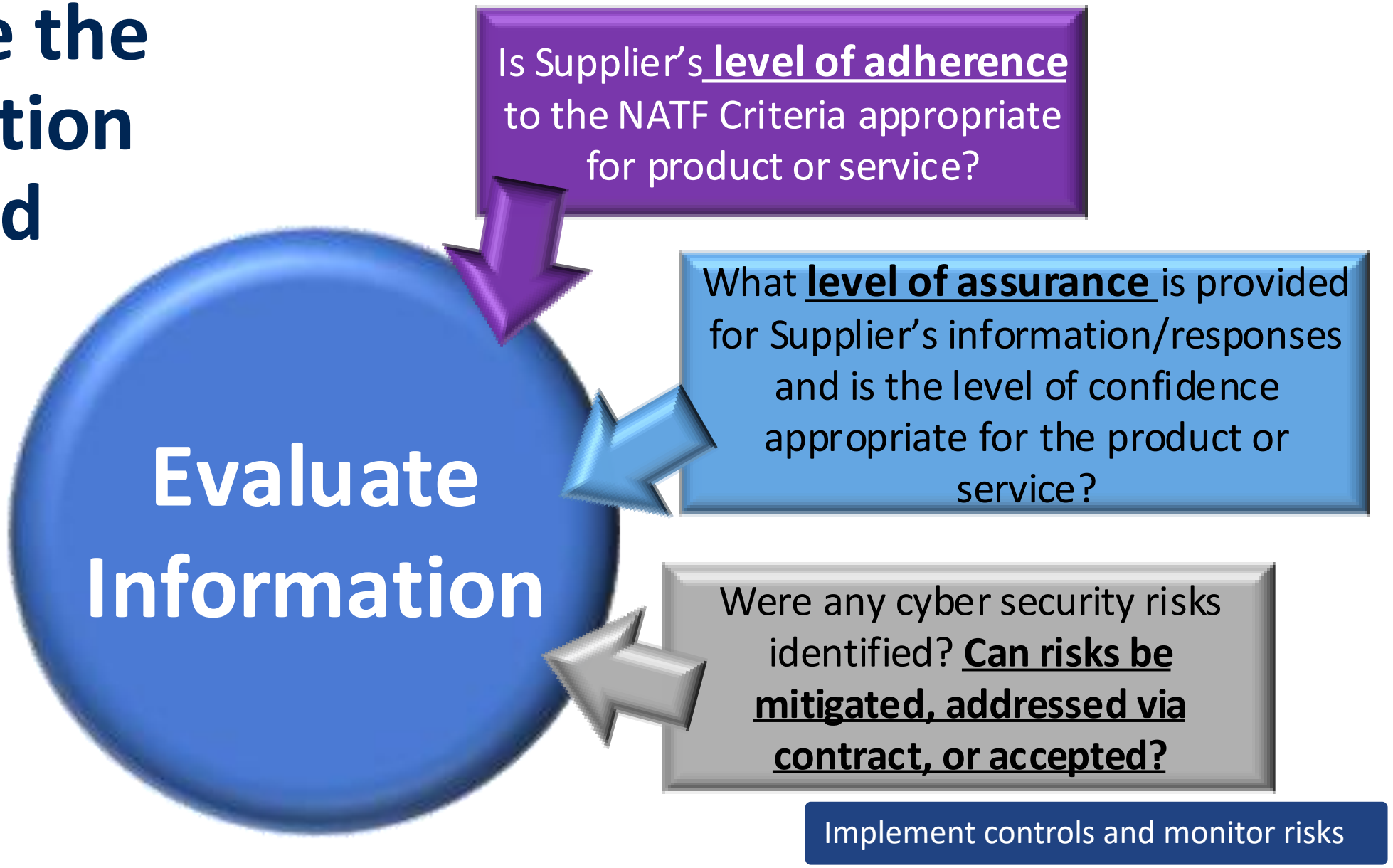


Implement Controls and Monitor Risks

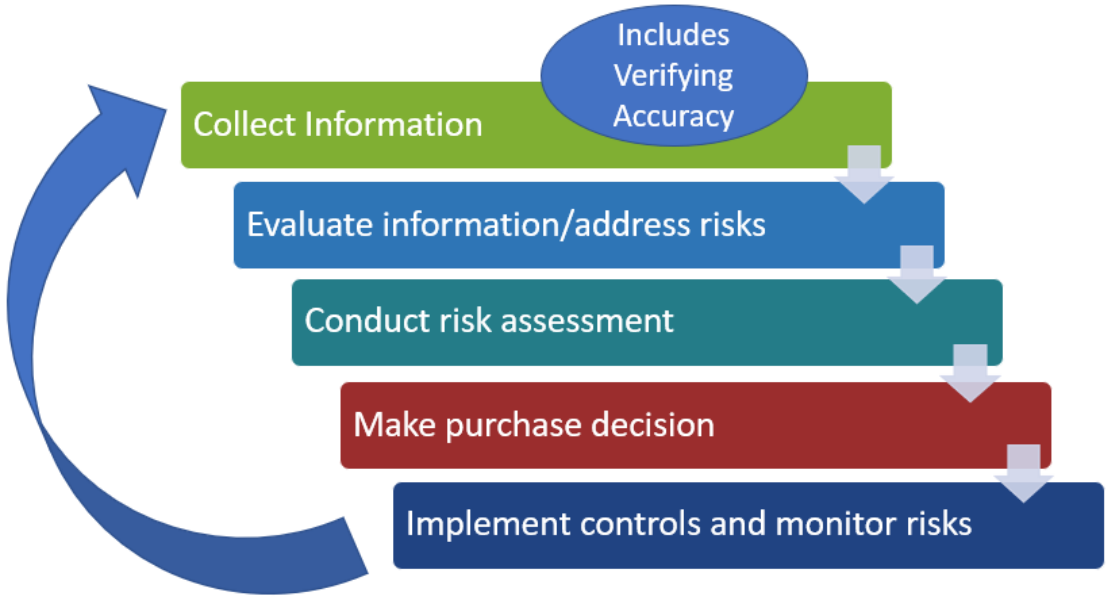
- Monitor risks and controls throughout the lifecycle of the products or services
- Monitor the supplier for changes that could affect products or services as well as breaches or compromises

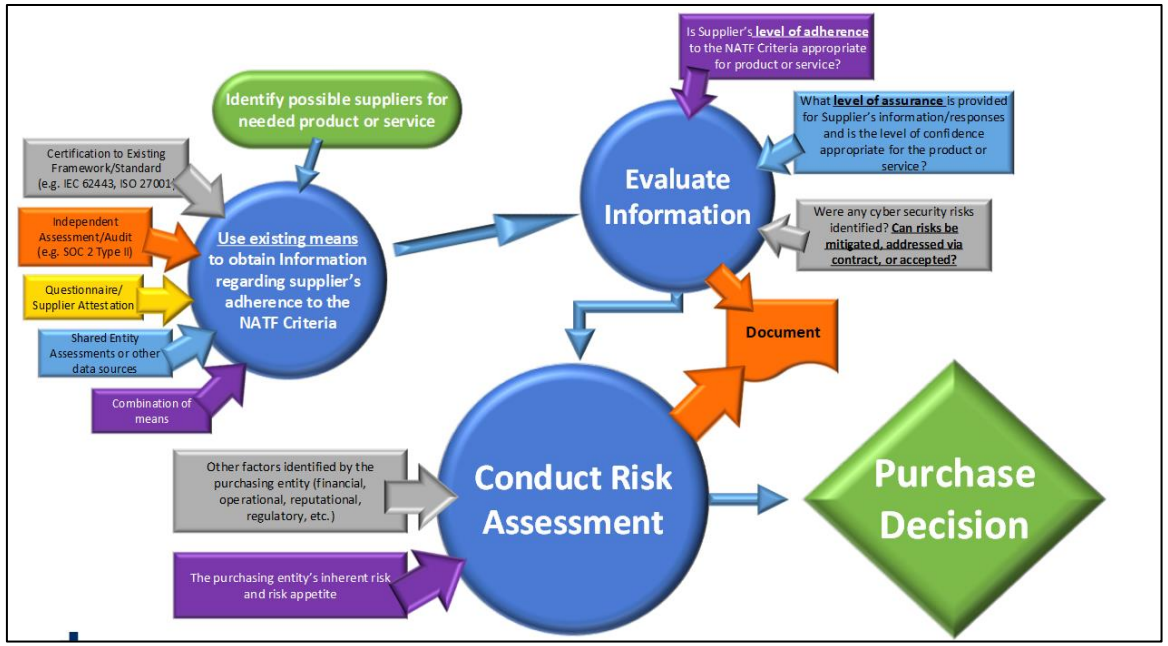
Implement controls and monitor risks

Evaluate the Information Obtained



Graphical Representations of The Model





North American Transmission FORUM

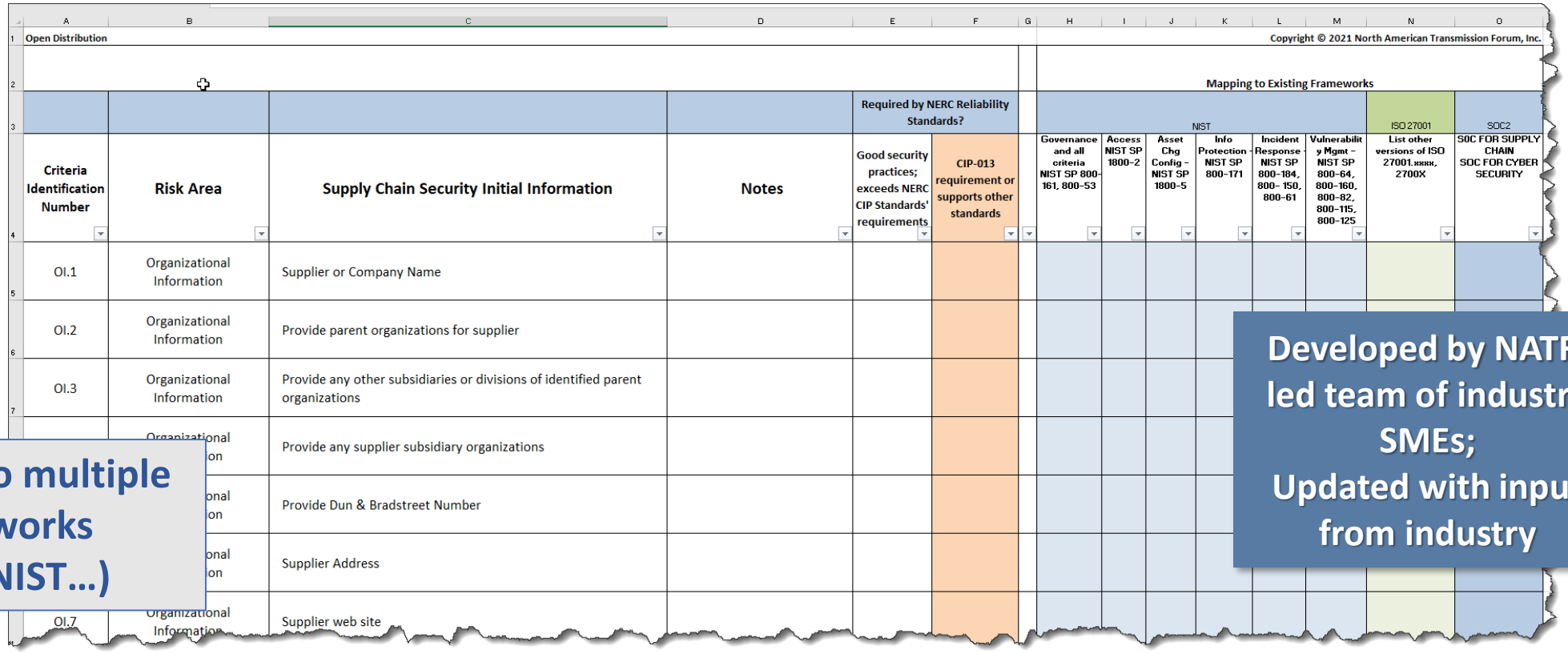
Tools

Available on the NATF Public Website:

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

NATF Supply Chain Security Criteria

Provides a basis for measuring a supplier's security posture/practices (i.e., a "best practices" list), which can also be used to collect information from a supplier



Open Distribution

Copyright © 2021 North American Transmission Forum, Inc.

				Required by NERC Reliability Standards?		Mapping to Existing Frameworks							
						NIST						ISO 27001	SOC2
Criteria Identification Number	Risk Area	Supply Chain Security Initial Information	Notes	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	List other versions of ISO 27001.xxxx, 2700X	SOC FOR SUPPLY CHAIN SOC FOR CYBER SECURITY
OI.1	Organizational Information	Supplier or Company Name											
OI.2	Organizational Information	Provide parent organizations for supplier											
OI.3	Organizational Information	Provide any other subsidiaries or divisions of identified parent organizations											
	Organizational Information	Provide any supplier subsidiary organizations											
	Organizational Information	Provide Dun & Bradstreet Number											
	Organizational Information	Supplier Address											
OI.7	Organizational Information	Supplier web site											

Maps criteria to multiple security frameworks (e.g., ISO, IEC, NIST…)

Developed by NATF-led team of industry SMEs; Updated with input from industry

NATF Supply Chain Security Criteria

63 criteria for supplier supply chain cyber security practices within 6 risk areas:

- ✓Asset control and management
- ✓Asset change and configuration management
- ✓Governance
- ✓Incident response
- ✓Information protection
- ✓Vulnerability management

24 organizational information considerations

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

Energy Sector Supply Chain Risk Questionnaire

Provides a consistent set of questions that support the NATF Criteria and help obtain more-granular information on a supplier's security risk performance

**Developed by NATF-led team of industry SMEs;
Updated with input from industry**

Energy Sector Supply Chain Risk Questionnaire - Unformatted						Version 1.0	Published 5/8/2020	
IAM-30	Do you have process(es) and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?							
Cybersecurity Program Management		**Supplier Corporate Systems**	**Supplier Product**	**Product Development**	**Additional Information**		**NATF Criteria**	**Primary or Supporting for NATF Criteria**
CSPM-01	Do you have a business continuity plan (BCP) to support ongoing operations of your systems and scope of equipment and/or services provided to the entity?						21	Primary (21) Supports (44)
CSPM-02	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?							Supports (21)
CSPM-03	Has your BCP been tested in the last year?							
CSPM-04	Does your organization have a data privacy policy that applies to your computing systems?							Supports (38)
CSPM-05	Have overall system and/or application architecture diagrams, including a full description of the data communications architecture, been developed and documented for the product(s) and/or service(s) being purchased?							Supports (56)
CSPM-06	Do you have a media handling process (that is documented and currently implemented), including end-of-life, repurposing, and data sanitization procedures?						40	Primary (40) Supports (2)
CSPM-07	Does your information protection program include secure deletion (e.g., degaussing/cryptographic wiping) or destruction of sensitive data, including archived or backed-up data?						46	Primary (46)
CSPM-08	Do you have third-party assessment(s) and/or certification(s) you have conducted to assess your cybersecurity practices? If yes, please describe the assessment or certification, date last completed, and frequency of re-assessment in the Additional Information column.					Provide the findings reports from third-party verifications conducted for cyber security frameworks (provide the two most recent reports for each cyber security framework).	24	Primary (24)
CSPM-09	Do you establish and maintain a security program for the your environment, including implemented processes to approve software, patches, and firmware prior to installation, as well as to verify the integrity and authenticity of the software, patches and firmware relevant to any technologies or equipment used in the development, manufacturing, testing, assembly, and distribution of the product(s) or service(s)?						54	Primary (54)

key supporting questions are identified

Energy Sector Supply Chain Risk Questionnaire

223 questions plus 19 general information questions in 12 categories:

- ✓Company Overview
- ✓Identity & Access Management
- ✓Change & Configuration Management
- ✓Mobile Devices & Application
- ✓Cybersecurity Program Management
- ✓Risk Management
- ✓Cybersecurity Tools & Applications
- ✓Supply Chain & External Dependencies Management
- ✓Data Protection
- ✓Vulnerability Management
- ✓Event & Incident Response
- ✓Workforce Management

Questions for 3 Areas:

- ✓Supplier Corporate Systems
- ✓Supplier Product
- ✓Supplier Development System

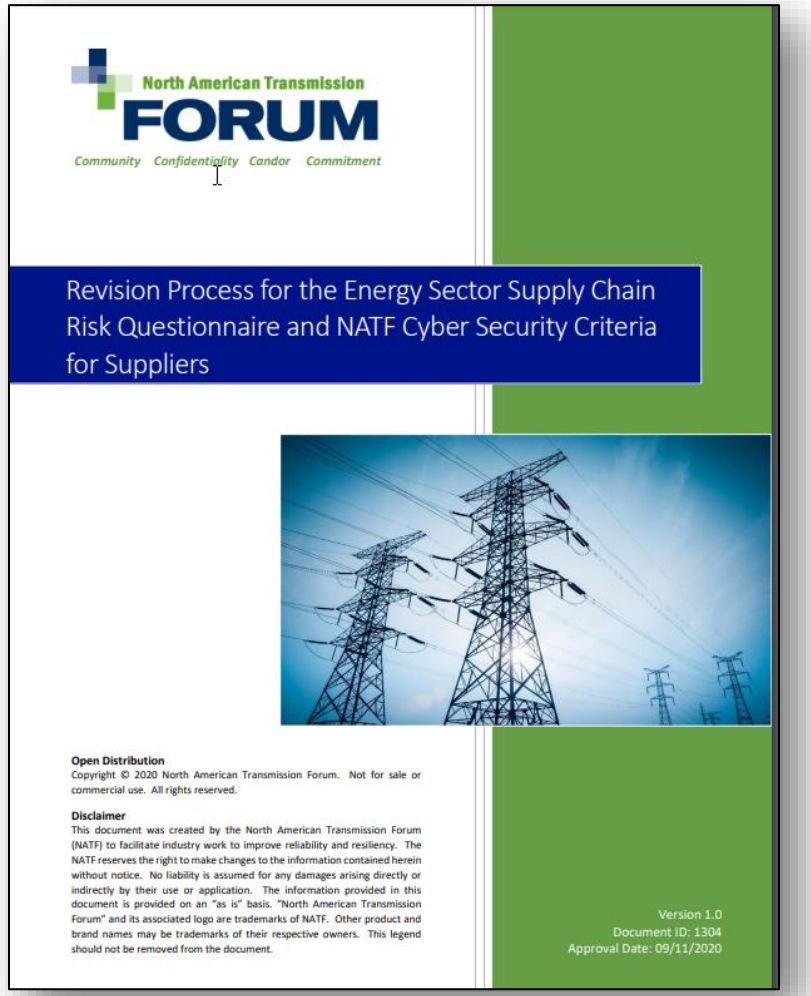
Posted on https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

Industry-wide Revision Process for Criteria and Questionnaire

Provides for an annual cycle to modify or update the Criteria and Questionnaire based on inputs from industry including utilities, suppliers, assessors, and other industry organizations

Intake of industry comments → **Consideration of comments** → **Modifications posted for comment** → **Comments resolved; modified Criteria or Questionnaire posted**

- **Annual cycle is in process**
- **Proposed changes are posted for industry comments through April 13**



Examples of Supply Chain Resources

NATF

- NATF Guidance for CIP-010-3 Software Integrity
- NATF CIP-013 Implementation Guidance – Independent Assessments of Vendors (ERO Endorsed)
- NATF CIP-013 Implementation Guidance – Supply Chain Risk Management Plans (ERO Endorsed)
- Large Entity Use Case (Webinar)

Solution Providers and Third-Party Assessors

- NATF Industry Collaboration: Using Solution Providers for Third-Party Risk Management
- Understanding Third-Party Assessments
- Suppliers Responding to Requests for Cyber Security Information (Webinar)

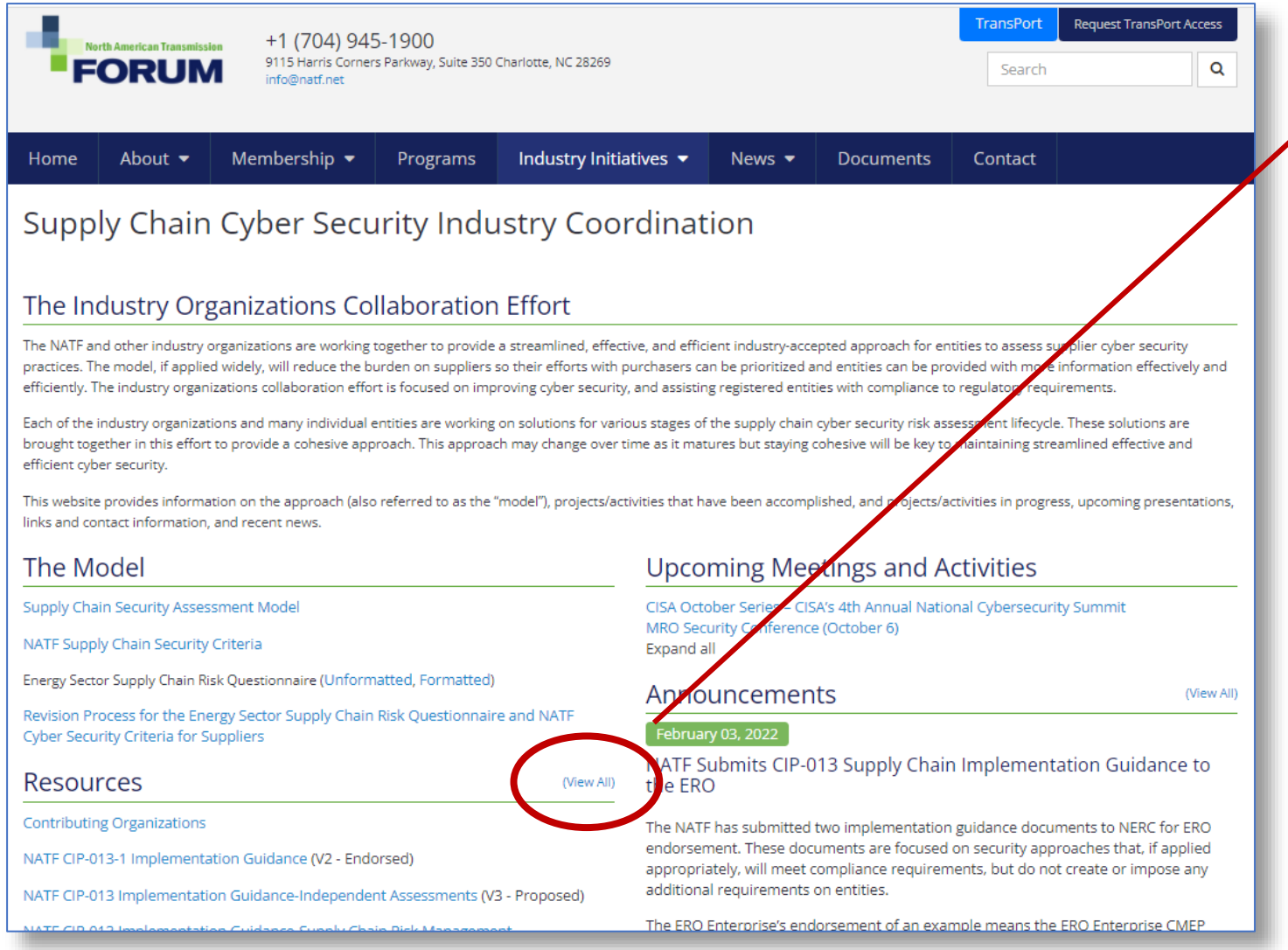
Trade Organizations, Forums and NERC Committees

- APPA's Cyber Supply Chain Risk Management (external)
- EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk V2
- NERC Supply Chain Working Group (SCWG) Security Guidelines
- Supply Chain Compliance Joint ERO and CCC Webinar 08072021 (Webinar)
- WEF: Advancing Supply Chain Security in Oil and Gas: An Industry Analysis

Available at:

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

NATF Public Website



Provides:

- Documents
- Presentations/Webinars
- Related Supply Chain sites
- Support Products and Services

Available at:

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

North American Transmission FORUM

The Value Proposition

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

NATF Supply Chain Security Assessment Model Value Proposition

Objectives

- Security
- Industry Convergence
- Efficiency and Effectiveness
- Compliance

Mitigation

Provides a foundation for entities to identify and mitigate supply chain risks

Partnerships

Provides opportunities for entities and suppliers to mitigate risks

Inclusive

Allows entities to work with current suppliers and third-party assessors

Adaptable

Open process to identify or modify needed information

Convergence

Identification of needed information allows suppliers to be responsive

Validation

Facilitates collection and verification of industry-specific information

Convergence

Effective and Efficient for Industry

- Convergence on information needed to evaluate risk
- Manageable amount of data

Effective and Efficient for Suppliers/Vendors

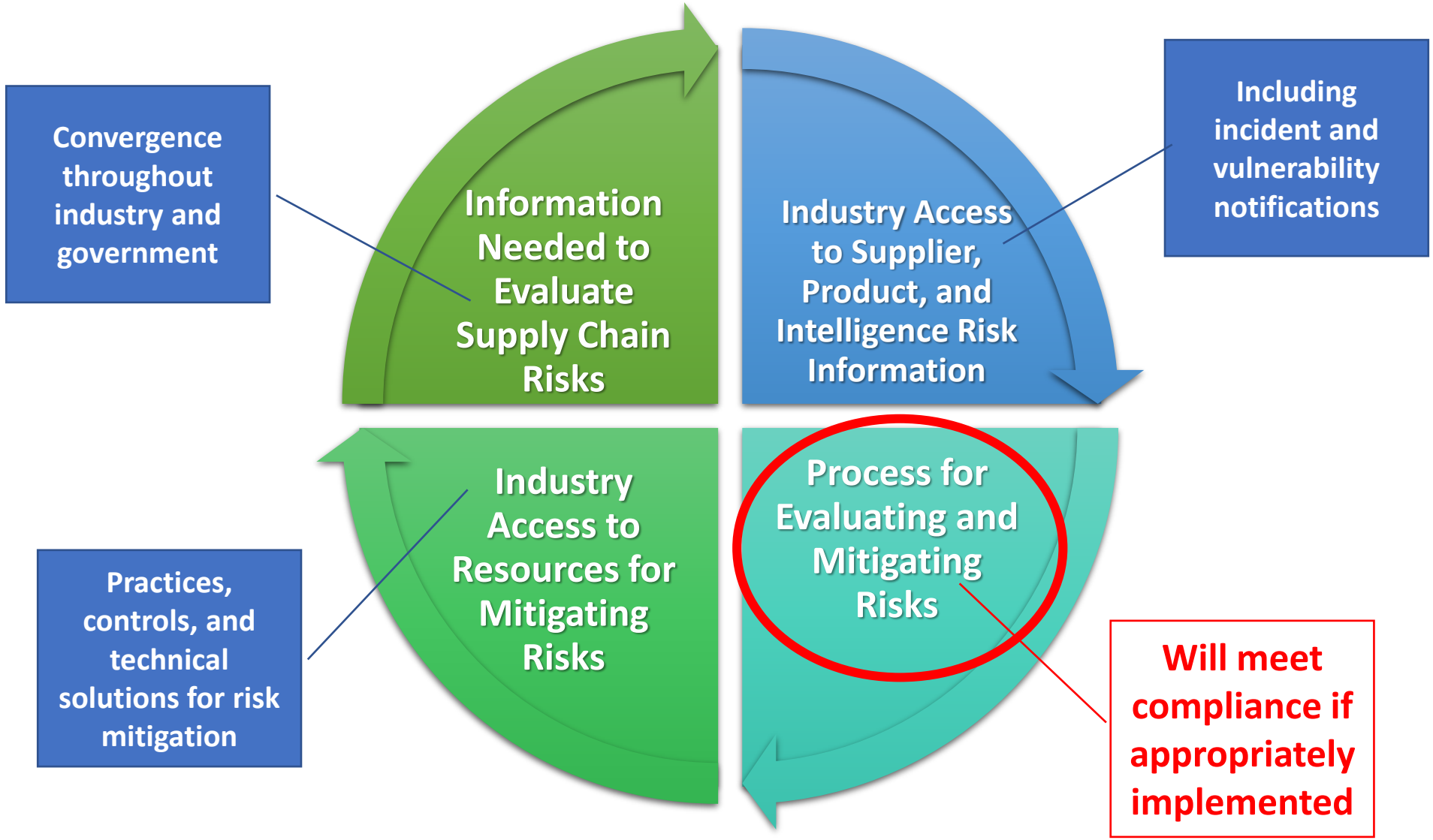
- Information consistency provides for faster vendor response

Validation of Supplier Information using Current Tools – Relying Upon the Work of Others

- Criteria are Mapped to Multiple Security Frameworks
  - Includes NIST, ISO 27001, IEC 62443 and SOC
  - NIST does not have an associated certification or assessment
- One framework does not cover all criteria
- Obtaining multiple certifications will cover most criteria

The Vision for Alignment

Key Components for Supply Chain Security



North American Transmission FORUM

Do you want to be included on an NATF external roster?

If yes, provide your name, company and email to:

supplychain@natf.net

Questions