North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

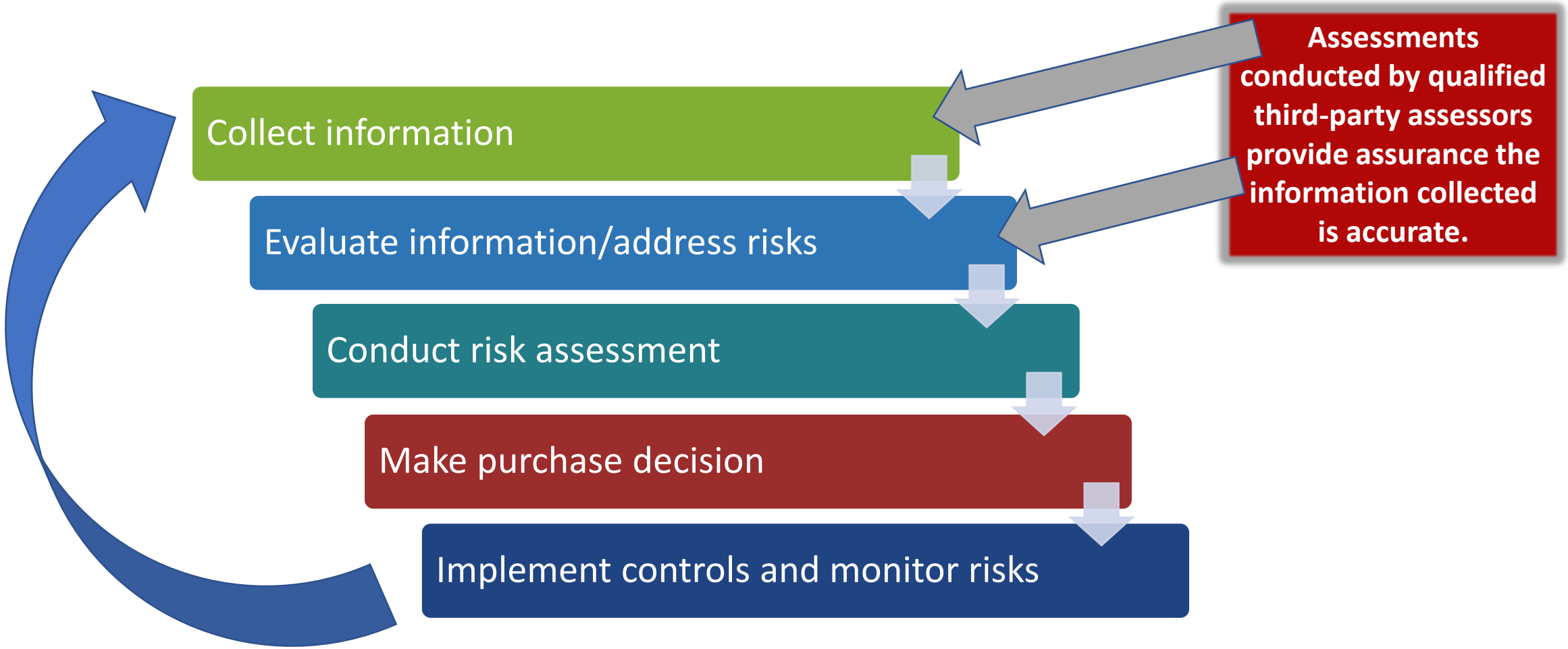
Understanding Third-Party Assessments

Deloitte, Ernst & Young, PricewaterhouseCoopers

Supplier Risk Assessment Challenges

- Greater reliance is being placed on outside technology suppliers
- Enhanced sophistication of cyber adversaries
- Supply chain and third-party cybersecurity risk is growing
- Number of risk assessments is increasing exponentially
- Regulations are expected to expand
- Increasing volume of alternative questionnaires received by suppliers
- Registered entities and suppliers are adding resources to support risk mitigation activities
- Lack of standardization creating inefficiencies

Registered Entity Risk Assessment Process



Supplier Risk Assessment Options

Third-Party SOC2 or SOC for Supply Chain Assessment

- Executed by independent third party
- Report includes detailed evidence of controls tested and results,
- Gaps are disclosed

Non-framework Based Third-Party Assessment

- Executed by independent third party
- Depth of assessment and reporting varies based on engagement scope
- Gaps are disclosed

External ISO Certification

- Executed by independent third party
- Provides summary level results of areas in scope
- May or may not include testing of controls
- Gaps are not typically disclosed

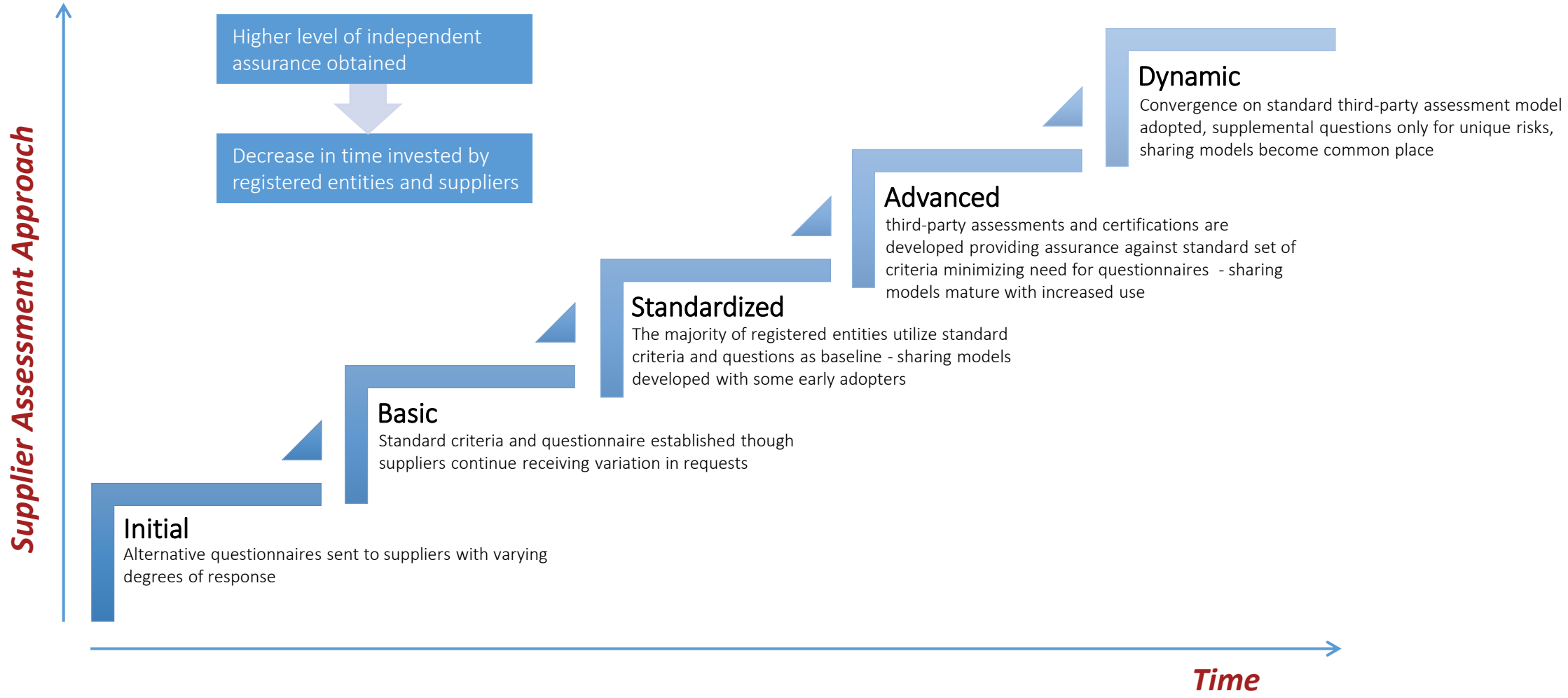
Internal ISO Certification

- Executed internally by objective company employee
- Provides summary level results of areas in scope
- Report excludes detail regarding controls tested and results

Questionnaire

- Effective way to obtain initial input regarding supplier's security posture
- Executed by company employees
- Supplier attests to meeting specified criteria

Supplier Risk Assessment Journey



Benefits of Industry Wide Third-Party Assessment Standard

- Industry wide adoption of a standard third-party supplier controls attestation report would offer…
  - A single document for suppliers to respond to requests
  - Consistent review process and risk assessment across organizations
  - Transparency regarding internal controls design, controls effectiveness and gaps
  - Robust easy report readability for both registered entities and suppliers
  - A solid framework to obtain assurance
  - Better understanding of performance expectations
  - Greater level of independent assurance

Why obtain a Third-Party Assessment?

A third-party assessment conducted by a qualified assessor will:

- **Provide an objective assessment**
- **Provide you with a high level of assurance the information the supplier provides you is accurate**
- **Reduce the amount of review your organization needs to conduct**
- **Provide evidence for compliance**

How do I obtain a Third-Party Assessment?

A registered entity or supplier determines what type of third-party assessment(s) they want to have performed

- A **qualified** assessor is selected to perform the activity

The qualified assessor issues a report or certificate

The supplier is reviewed periodically to ensure the certification or opinion is valid

Qualified Assessors

- **ISO Certifications**
- The ANSI National Accreditation Board (ANAB) is a non-governmental organization that provides accreditation services and training to public- and private-sector organizations, serving the global marketplace. ANAB is the largest accreditation body in North America and provides services in more than 75 countries. Accredited organizations can be identified here: http://anabdirectory.remoteauditor.com/

- **SOC Reports**
- Must be a licensed Certified Public Accountant (CPA) firm with the AICPA. Can be identified by State Board of Accountancy website or https://cpaverify.org/
- Important the firm has resources who are experienced with information technology and security audits and have relevant certifications (e.g., CISA, CISSP)

How would I use a Third-Party Assessment to Evaluate a Supplier?

The NATF has developed Criteria for you to use in evaluating a supplier's cyber security practices

- The NATF Criteria Spreadsheet contains a mapping for many frameworks to the NATF Criteria; you can add additional frameworks
- Use the Supplier Assessment Model to identify any supplier risks
  - The third-party assessment brings assurance NATF criteria are met
  - Product or service risk informs level of comfort needed by the third-party assessment
  - Different types of third-party assessments provide varying levels of comfort

Statement of Applicability (SOA)

- If obtaining a certification obtain an SOA to ensure applicability. An SOA is not necessary if a SOC2 or SOC for Supply Chain report is available.
- The SOA is a controlled document that provides an overview of the implementation of a security framework. It addresses:
    1. Entity (locations within the entity) and the scope of business operations
    2. The relevant controls and objectives
        - What controls are deemed in scope and why
        - What controls are deemed out of scope and why
    3. The security controls in place to achieve the controls deemed in scope.
- It is approved by management and typically reviewed annually or updated out of cycle if there is major change in operations.

Appendix

Comparison of Common Reporting Frameworks

Description	ISO	SOC2
Purpose	Certification supporting compliance with ISO requirements covering security management.	Reporting on controls relevant to security as well as other optional areas: availability, processing, integrity, confidentiality, privacy and/or supply chain activities.
Framework	Internationally agreed upon standards covering information security developed by the The International Organization for Standards (or "ISO"). The ISO 27001 standards were established to help organizations manage their security of assets.	SOC 2 is a reporting framework that is flexible enough to cover a wide variety of information processing objectives related to the categories noted above. It is not bound by a single "information security framework" (e.g. ISO, NIST, etc), so organizations can adopt SOC2 reporting regardless of the information security framework they've used to implement security practices within their unique environment.
Report Users	General use and can be freely distributed to all the stakeholders.	Restricted use. Distribution of company's customers and other stakeholders (e.g. regulators).
Process Output	Certificate of Conformity/Registration (Compliance)	Detailed service auditor's report with opinion
Certification Process	Company personnel or third-party assessor who is accredited by ISO	Attestation by a firm approved by the AICPA
Organization Specific Controls	No - assessment against standards.	Yes - service organization describe the controls to be disclosed in the service auditor's report.
Certification or Opinion	Certification	Audit Opinion

Comparison of Common Reporting Frameworks *(cont.)*

Description	ISO	SOC2
Intended Focus	Providing insight into the process that management uses to operate the Information Security Management System (ISMS) to meet ISO standards.	Providing insight into the effectiveness of the control environment through reporting on the results of design and operating effectiveness testing of specific controls.
Contents of the Report	Certification supporting conformance with ISO requirements. The report does not include specific controls at the organization, tests performed, or the results of tests performed. Gaps identified by a third-party assessor are not disclosed. If an entity does not close gaps within a specified period of time the entity loses its certification, however those details are not disclosed to the recipients.	SOC2 reports include a detailed description of the processing environment within the scope of the report. In addition, the report clearly lays out: - Specific controls at the organization - Tests performed by the independent auditor - Results of the tests performed by the independent auditor Gaps are disclosed and may result in a qualified opinion, which affects the user organization's ability to rely on supplier controls.
Report Detailed Testing & Results	No	Yes - Report includes detailed test plans and results for each test. Type 1 report will cover a point in time (e.g., as of December 31) and Type 2 will cover a period (e.g., January 1 through December 31).
Frequency and period covered	ISO certifications generally are issued on an annual basis; however, may be issued more or less frequently. Certification only covers a point in time (i.e., effective date). Certifications typically have an expiration date; however, this does not mean work was performed beyond the effective date.	SOC2 reports generally are issued on an annual basis; however, there is flexibility in length of time covered in the report, particularly in the first year (can be as short as 6 months of coverage prior to the report date)
Coverage?	Typical certification is at the product level though ISO provides flexibility in coverage.	SOC2 generally provides broader coverage for products and locations supported by common or individually designed controls.