

Third Party Information Security Risk Management Programs

Tanya Scott

Risk and Controls Program Manager, Autodesk

In-Depth Seminars – D33

Session Objectives / Agenda

Objectives

- Obtain insight into Third Party Information Security Risk Process and Tools
- Acquire tips and tricks (techniques) for implementing a new program or improving an existing program

Agenda

- Overview
- Establishing the Program's Foundation
- Executing the Program
- Continuously Improving the Program
- Wrap Up / Questions

Overview

Establishing the Program's Foundation

Executing the Program

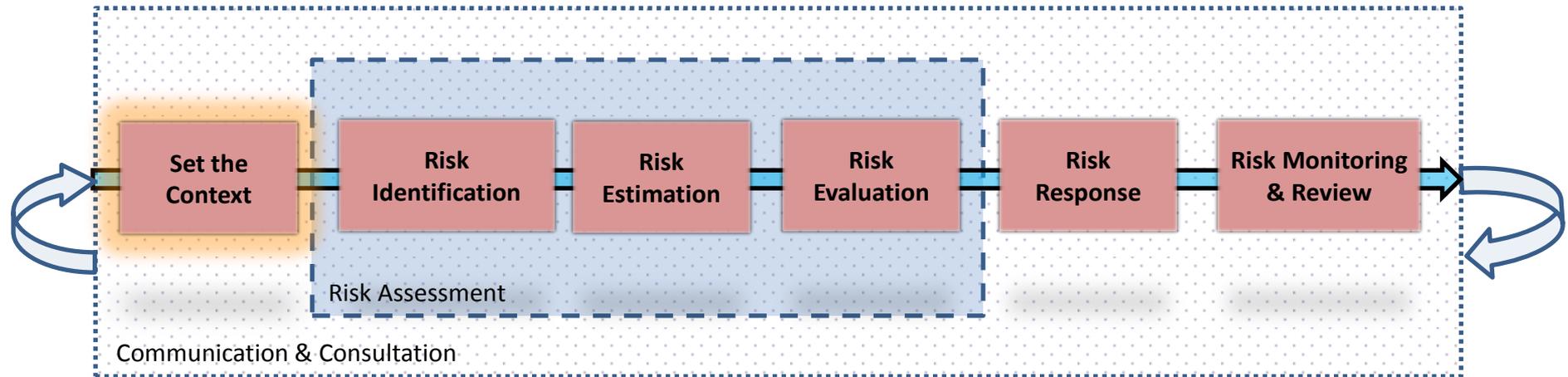
Continuously Improving the Program

Wrap Up / Questions



Third Party Information Security Risk Management

Setting the Context



- **ISO 31000** - Principles, Framework, Process
- **Risk** – *the effect of uncertainty on objectives*

Tackling Third Party Information Security Risk...

An Infinite Journey

Establishing the Program's Foundation

- Defining the Purpose
- Developing the Baseline
- Gaining Buy-In and Support

Executing the Program

- Utilizing Tools and Reporting



Continuously Improving the Program

- Assessing the Program, Identifying and Remediating Gaps

Overview

Establishing the Program's Foundation

Executing the Program

Continuously Improving the Program

Wrap Up / Questions



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Defining the Purpose of the Program

Consider...

- Why is the team performing the assessments?
- What will the process / efforts lead to?
- What is the value proposition?
- What is the vision?
- What is the culture ready for?
- Which third parties are in-scope?
- What third party risks are focused on?
- Who is involved/impacted?
- Who is responsible/accountable?
- When will this effort occur?
- Who is the sponsor?
- How often will the process be assessed?
- How often will the team report out on risk?

Developing the Baseline - Defining “Third Party”



Developing the Baseline - “Good Practice”

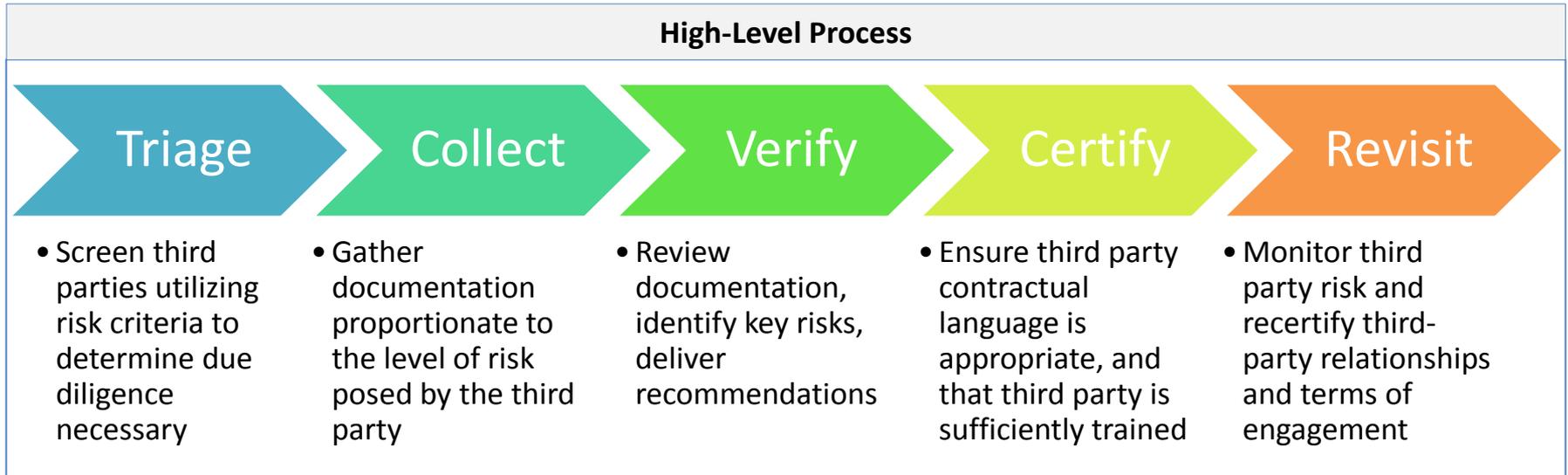
Several resources available:

- COBIT 5
- COBIT 5 for Information Security
- COBIT 5 for Risk
- Corporate Executive Board
- Gartner
- Forrester
- GRC Vendors
- Consultants and/or Auditors
- LinkedIn Groups, Blogs



Developing the Baseline – Example

High Level Process and Program Objectives



Key Program Objectives	
<ul style="list-style-type: none"> ➤ Supporting Policies, Standards ➤ Common Language, Process ➤ Clear Roles and Responsibilities ➤ Early Involvement of Relevant Parties ➤ Risk Levels and Necessary Due Diligence Defined ➤ Refined Questionnaire 	<ul style="list-style-type: none"> ➤ Automation, Increased Efficiency and Ease of Use ➤ Central Document Repository ➤ Simplified Final Reports, Info to Business Owners ➤ Tracking of Vendors, Remediation, Reassessments ➤ Increased Awareness ➤ Metrics and Reporting

Developing the Baseline – Example

Process Phases, Key Activities, Ownership

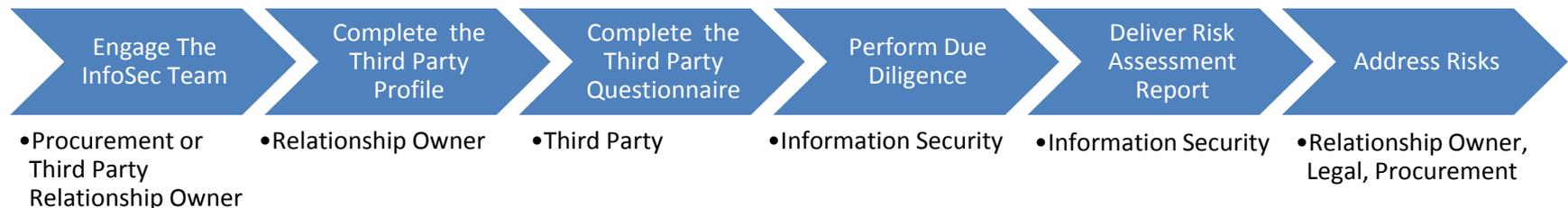
Triage		Collect		Verify		Certify		Revisit	
Key Activities	Typical Owners	Key Activities	Typical Owners	Key Activities	Typical Owners	Key Activities	Typical Owners	Key Activities	Typical Owners
Identify all existing relationships	Procurement , Business	Establish Documentation requirements	Legal	Analyze collected data	InfoSec	Define contractual protections	Legal, Procurement	Monitor changes	Relationship Owner, InfoSec
Develop risk criteria	Legal, InfoSec	Deploy questionnaire to third party	Relationship Owner	Identify Risks and Deliver Executive Report	InfoSec	Require code of conduct Certification	Relationship Owner	Recertify regularly, Validate Remediation	Procurement, InfoSec
Assign a relationship owner	Business	Compile Documentation .	Relationship Owner, Legal, InfoSec	Approve third party or terminate due diligence.	Relationship Owner, Legal	Train third-party employees	Legal, Relationship Owner	Tailor recertification Diligence	Legal, InfoSec
Complete Third Party Profile	Relationship Owner			Drive Remediation Efforts with Third Party	Legal, Relationship Owner	Monitor open remediation items	Relationship Owner	Reassess risk Exposure	InfoSec
Determine Triage Risk Rating	InfoSec, Legal							Renew Contract or terminate relationship	Relationship Owner, Legal, Procurement

Gaining Buy-In and Support

Simplified Messages and an Intranet Site

Intranet Site Contents

- Process Overview
- Roles and Responsibilities
- Documentation Repository
 - Third Party Profile
 - Third Party Questionnaire
 - Completed Assessments
- FAQs
- Contact information



Gaining Buy-In and Support

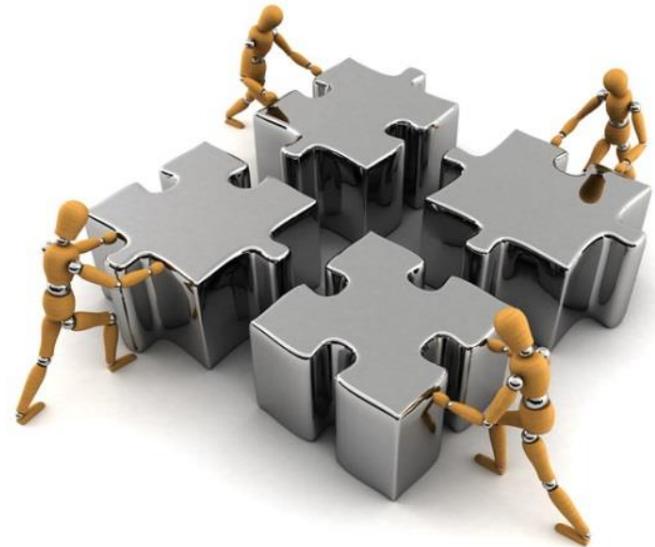
Policy and Standard Considerations

- Clear roles and responsibilities
- Third party relationship owners must:
 - ensure risk assessments are conducted prior to contracting with or onboarding a third parties
 - address identified information security risks
 - ensure that adequate provisions are included within the terms and conditions of the signed contract
 - ensure that a signed contract is in place prior to granting physical access to locations or logical access to information and systems
 - monitor third party service or contract changes that affect information security, and report such changes
 - ensure that the third party complies with applicable information security requirements as defined in the contract (including upon termination)

Gaining Buy-In and Support

Training the Team Responsible for Assessments

- Provide Training Sessions
- Provide Tools, Examples
- Periodically Review Deliverables
- Iterate!
- Measure



Overview

Establishing the Program's Foundation

Executing the Program

Continuously Improving the Program

Wrap Up / Questions



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

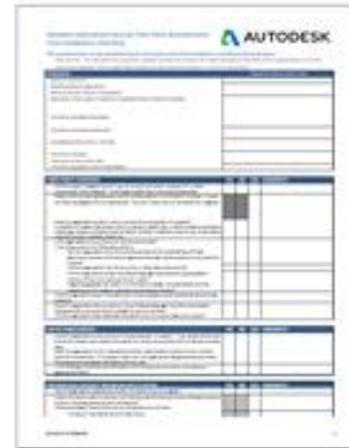
Executing the Program Tools Overview



1. Third Party Profile / Triage Assessment



2. Due Diligence Matrix



3. Third Party Questionnaire



4. Risk Report

STEP 1: Initial Assessment of Third Party Criticality

STEP 2: Gather Documentation and Conduct Due Diligence

STEP 3: Document and Deliver Risk Report to the Business

STEP 4: Remediation

STEP 5: Reassess

5. Document Repository / Tracking List

6. Risk Register

7. Third Party Risk Metrics

Third Party Profile / Triage Assessment

- What it is
- Why it adds value
- Who is involved
- Considerations

The image shows a screenshot of a 'Third Party Assessment' form from Autodesk. The form is titled 'Third Party Assessment' and includes the Autodesk logo. It is a structured document with several sections and a table for data entry.

Section 1: General Information

- Name of the Third Party: _____
- Address: _____
- City/State/Zip: _____
- Country: _____
- Phone: _____
- Fax: _____
- Website: _____
- Primary Contact Name: _____
- Primary Contact Title: _____
- Primary Contact Email: _____
- Primary Contact Phone: _____

Section 2: Business Information

- Business Type: _____
- Business Description: _____
- Year Founded: _____
- Number of Employees: _____
- Annual Revenue: _____
- Number of Customers: _____
- Number of Suppliers: _____
- Number of Franchises: _____
- Number of Licenses: _____
- Number of Patents: _____
- Number of Trademarks: _____
- Number of Inventions: _____
- Number of Products: _____
- Number of Services: _____
- Number of Markets: _____
- Number of Countries: _____
- Number of States: _____
- Number of Cities: _____
- Number of Regions: _____
- Number of Countries: _____
- Number of States: _____
- Number of Cities: _____
- Number of Regions: _____

Section 3: Risk Assessment

Risk Category	Score
Financial Stability	_____
Operational Stability	_____
Legal Compliance	_____
Reputation	_____
Other Considerations	_____

Section 4: Summary

Overall Risk Rating: _____

Assessment Date: _____

Assessor Name: _____

Assessor Title: _____

Assessor Email: _____

Assessor Phone: _____

Third Party Questionnaire

- What it is
- Why it adds value
- Who is involved
- Considerations

The image shows a screenshot of an Autodesk Third Party Questionnaire form. The form is titled "Autodesk Information Security Third Party Questionnaire" and includes the Autodesk logo. It is a structured document with several sections, each containing text and a table for data entry. The sections are:

- Company Information:** A table with columns for Name, Address, City, State, and Country.
- Product/Service Information:** A table with columns for Product/Service Name, Description, and Version.
- Security Information:** A table with columns for Security Measures, Risk Assessment, and Incident Response.
- Compliance Information:** A table with columns for Compliance Standards, Audit Frequency, and Audit Results.
- Other Information:** A table with columns for Other Information, Contact Person, and Contact Information.

Third Party Risk Report

- What it is
- Why it adds value
- Who is involved
- Considerations

AUTODESK
Information Security
Third Party ABC, Service Offering/Team

Assessment Details
Assessment Date: November 19, 2013
Approved By: [Name]
Reviewed By: [Name]
Reviewed For: Information Security / Information Security / [Name]

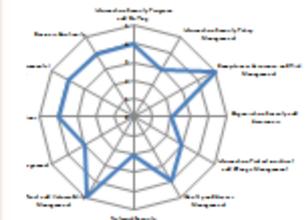
Assessment Summary
The risk matrix is created by analyzing third party's capability into the Organizational Platform. The capability which cannot be able even to see that having satisfactory evidence of the third-party service provider the feedback. Further on details to help with Autodesk third party's support to the Organizational Platform. Risk matrix is regularly provide updated information about to the team and generally can include the updated risk or condition and change.

Risk Matrix

	Opportunities	Risks
High	Low	High
Low	Low	High

Findings

- Findings about the [Name] [Name]
- Findings about the [Name] [Name]
- Findings about the [Name] [Name]



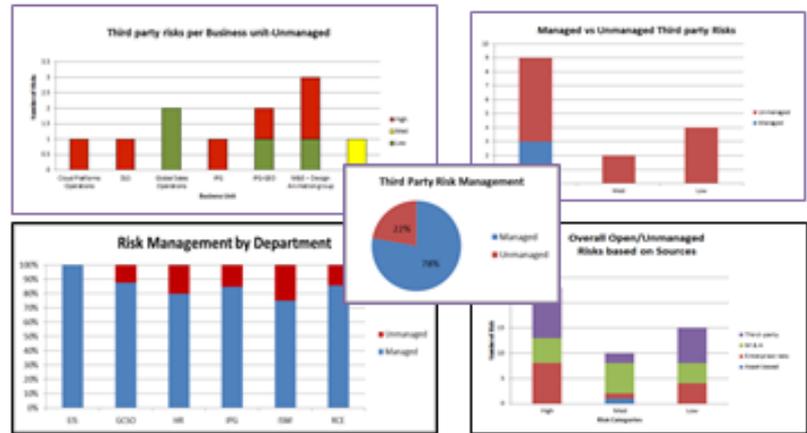
Risk	Impact	Likelihood	Mitigation
High	High	High	[Mitigation]
Low	Low	Low	[Mitigation]

Findings

- Findings about the [Name] [Name]
- Findings about the [Name] [Name]
- Findings about the [Name] [Name]

Third Party Risk Reporting / Metrics

- What it is
- Why it adds value
- Who is involved
- Considerations



Overview

Establishing the Program's Foundation

Executing the Program

Continuously Improving the Program

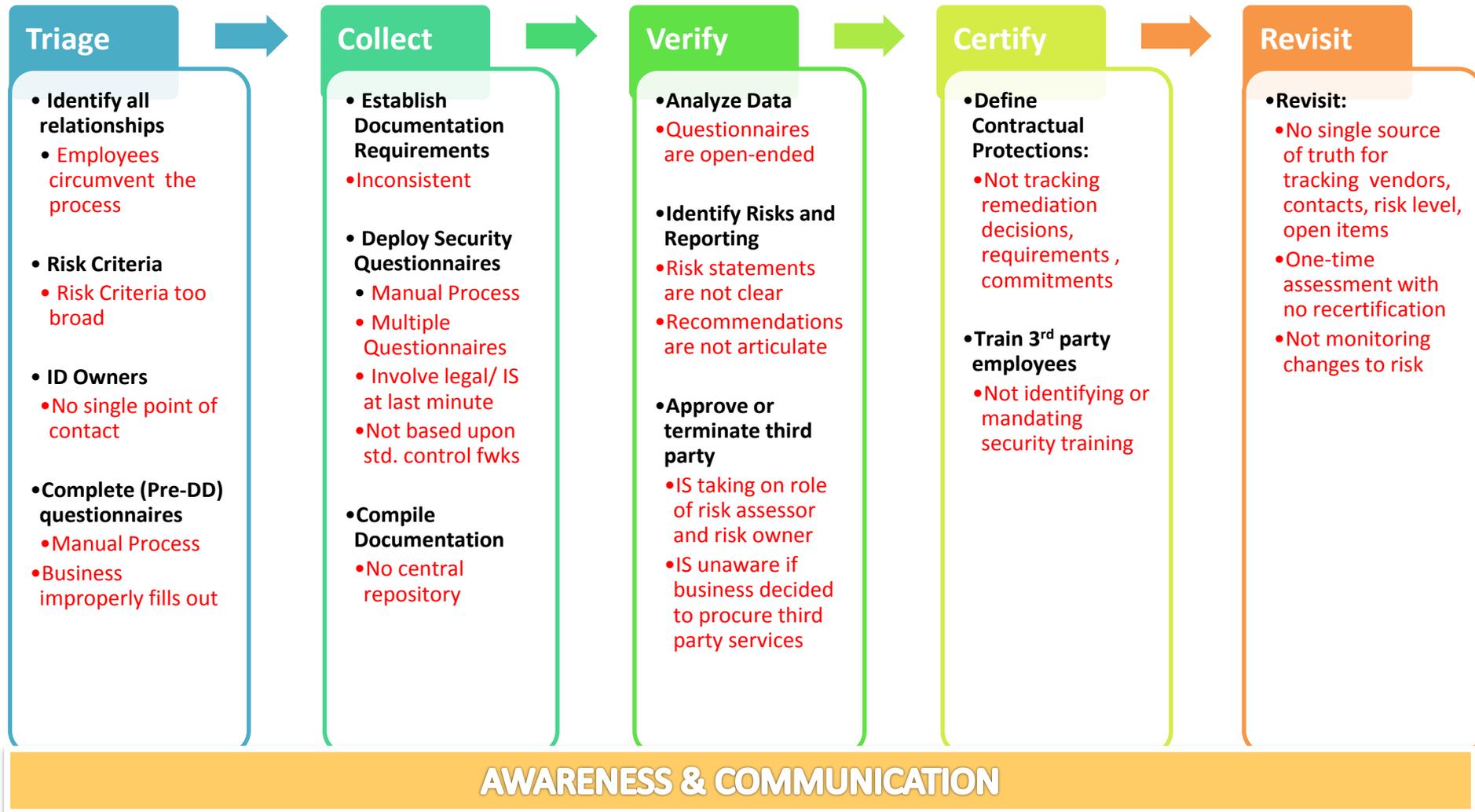
Wrap Up / Questions

Continuously Improving the Program

Assessing Current State – A Game Plan

- Revisit the Baseline
- Review Metrics, Risk Register, Reports
- Interview all Stakeholders Involved
- Document Existing Process(es)
- Inquire of Desires, Wish List
- Document the Gaps

Identifying Gaps with Current Process - Example



Overview

Establishing the Program's Foundation

Executing the Program

Continuously Improving the Program

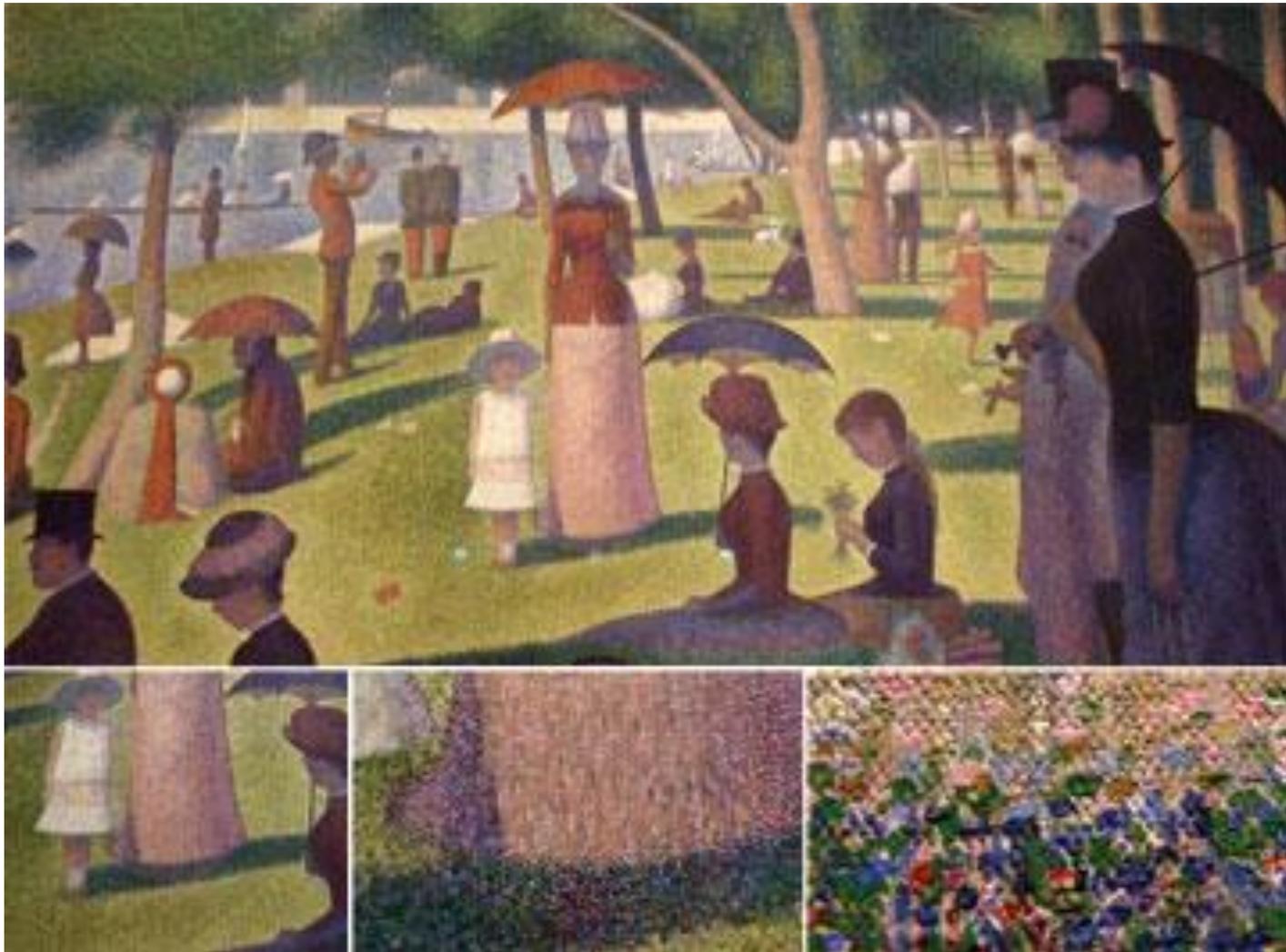
Wrap Up / Questions



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Final Comments



Questions?

Thank you!

Tanya Scott

Tanya.Scott@Autodesk.com