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

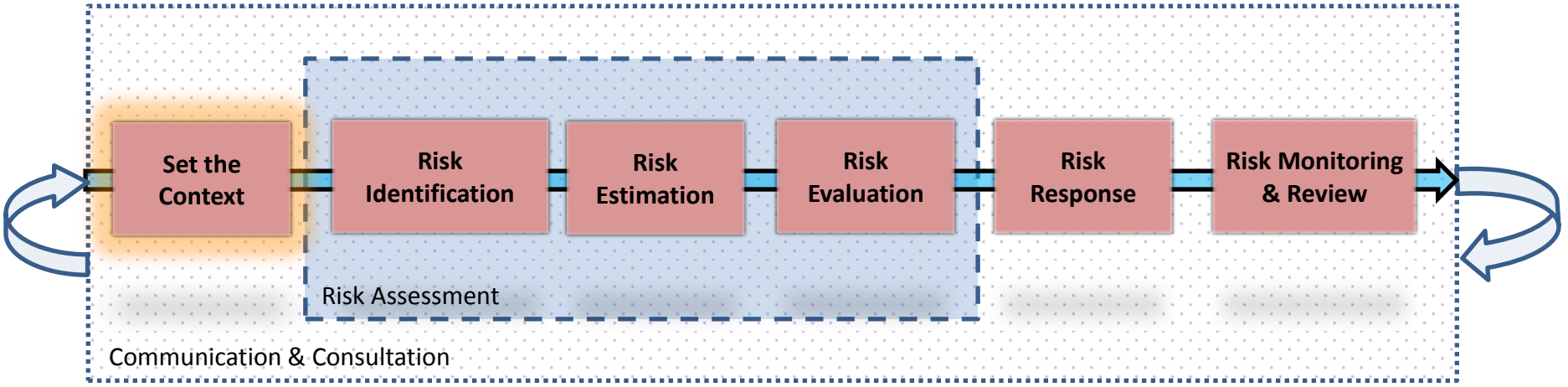
Establishing the Program's Foundation

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

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

High-Level Process

- **Triage**
  - Screen third parties utilizing risk criteria to determine due diligence necessary
- **Collect**
  - Gather documentation proportionate to the level of risk posed by the third party
- **Verify**
  - Review documentation, identify key risks, deliver recommendations
- **Certify**
  - Ensure third party contractual language is appropriate, and that third party is sufficiently trained
- **Revisit**
  - Monitor third party risk and recertify third-party relationships and terms of engagement

Key Program Objectives

- Supporting Policies, Standards
- Common Language, Process
- Clear Roles and Responsibilities
- Early Involvement of Relevant Parties
- Risk Levels and Necessary Due Diligence Defined
- Refined Questionnaire
- 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

Engage The InfoSec Team	Complete the Third Party Profile	Complete the Third Party Questionnaire	Perform Due Diligence	Deliver Risk Assessment Report	Address Risks
•Procurement or Third Party Relationship Owner	•Relationship Owner	•Third Party	•Information Security	•Information Security	•Relationship Owner, Legal, Procurement

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

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

Due Diligence Matrix

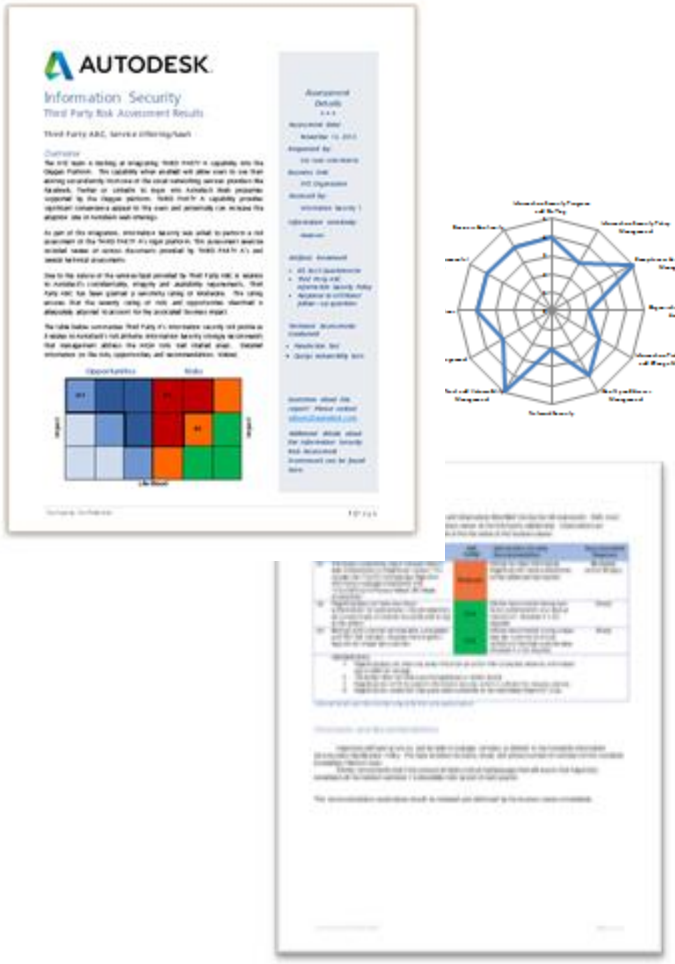
- What it is
- Why it adds value
- Who is involved
- Considerations

Third Party Questionnaire

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

Third Party Risk Report

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



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

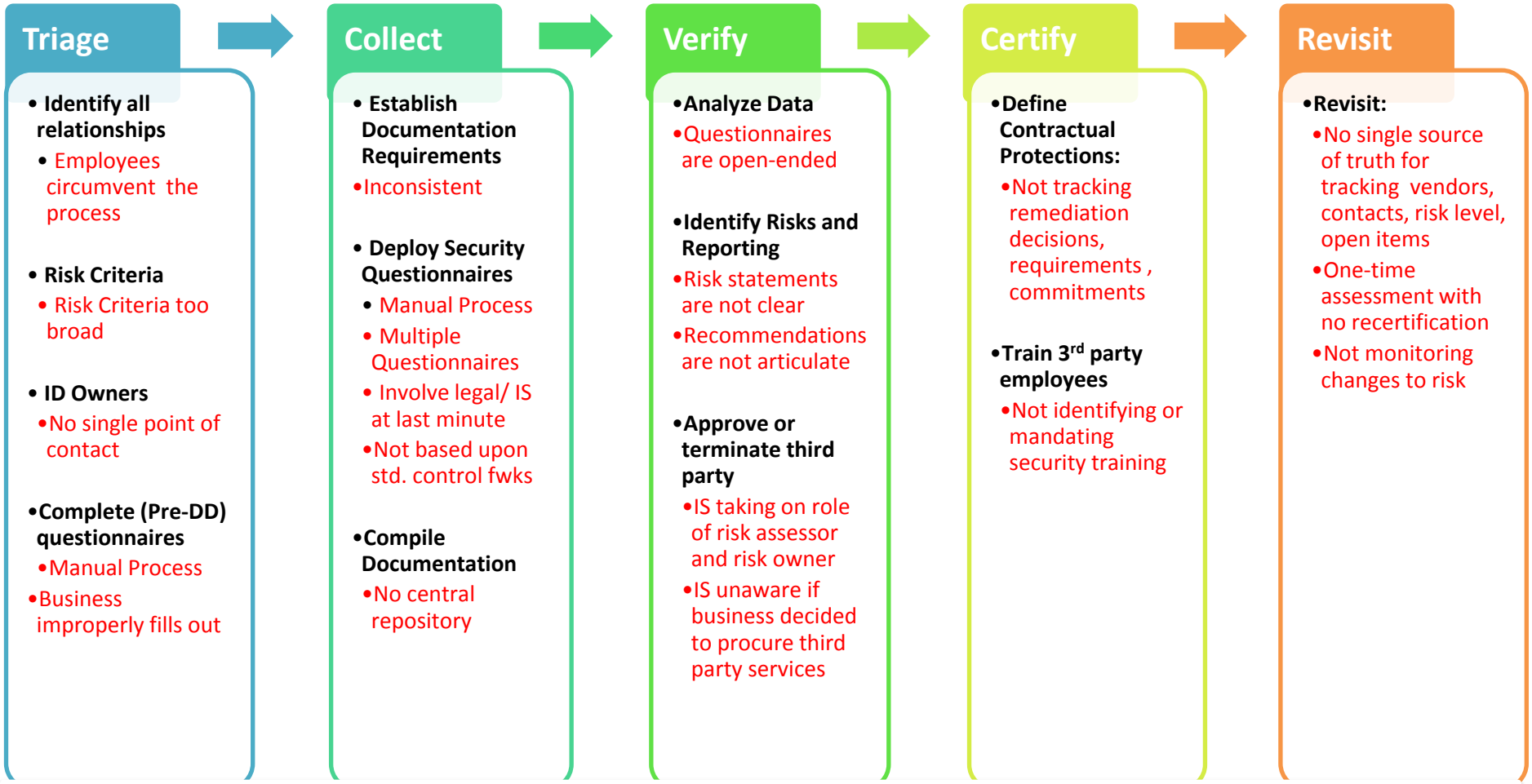
Continuously Improving the Program

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

Final Comments

Questions?

Thank you!

Tanya Scott

Tanya.Scott@Autodesk.com