

SAMANTHA TORREZ

Many Birds, One Stone: Using Asset-Based Risk Assessments for More Than Your Assets



KEYS
CONFERENCE

1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.

Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.

Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.

Unauthorized release of this information is prohibited.

Original material is copyright © 2022 Tandem.



KEYS
CONFERENCE

2



Samantha Torrez

CSXF, Tandem Software Specialist



3

Agenda

MANY BIRDS, ONE STONE

- Why use ABRA's?
- Custom Fields
- Third-Party
- Business Applications
 - Associations
- Departments
 - Data Classifications & Data Types
- Create Your Own "Template"



4



Why Use Asset-Based Risk Assessments?

MANY BIRDS, ONE STONE

5

Benefits of Asset-Based Risk Assessments

WHY USE ASSET-BASED RISK ASSESSMENTS?

- Define Your Assets
- Customize Data Types & Data Classifications
- Associate with Third Parties, Systems/Equipment, and Software
- Custom Fields
- Build Threats and Controls



6

What should I put in Custom Fields?

WHY USE ASSET-BASED RISK ASSESSMENTS?

- Checkbox
- Date
- Dropdown List (One or Multiple)
- Integer
- Plain Text
- Rich Text

Audit Frequency ⓘ

18 Months ▼

Asset Type ⓘ

Hybrid ▼

Physical Location ⓘ

DFW Branch

☐

Required

☒

Include field in applicable document downloads

☒

Include field in applicable spreadsheet exports



7



Third-Party Risk Assessments

MANY BIRDS, ONE STONE

8

Who are my third-parties?

THIRD-PARTY RISK ASSESSMENTS

- External relationships that provide a service
 - Contracted Services
 - Non-Contracted Services
- Third parties include:
 - CoNetrix / Tandem
 - Core Provider
 - ATM Services



Document your external relationships



Think about which service providers may warrant a risk assessment.



9

Threats and Controls for Third Parties

THIRD-PARTY RISK ASSESSMENTS

- **Threats**
 - Data Exposed to Other Customers
 - Loss of Connectivity
 - Operational Risk
 - Reputation Risk
- **Controls**
 - Secure Coding Techniques
 - Review Security Testing Reports
 - Data Loss Prevention (DLP) Program
 - Vendor Contract



10



Business Application Risk Assessments

MANY BIRDS, ONE STONE

11

BUSINESS APPLICATION RISK ASSESSMENTS

"A software used by business users to perform a business function or support a business capability."

Understanding Business Applications: Sankhadeep Dhar



12

Business Application Examples

BUSINESS APPLICATION RISK ASSESSMENTS

- Billing System
- Office 365
- File Storage
- CRM (Customer Relationship Management)
- SAP (Systems, Applications & Products in Data Processing)



13

Threats & Controls for Business Applications

BUSINESS APPLICATION RISK ASSESSMENTS

- | | |
|--|---|
| <ul style="list-style-type: none"> • Threats <ul style="list-style-type: none"> • Exploitation by Cyber Attack • Supply Chain Attack • Improper Licensing • Unauthorized Intentional Disclosure | <ul style="list-style-type: none"> • Controls <ul style="list-style-type: none"> • Intrusion Detection / Prevention System • Vulnerability Scans • Vendor Management Program • Logical Access Controls |
|--|---|









14

Utilize your Asset “Associations”

BUSINESS APPLICATION RISK ASSESSMENTS

Associations ⓘ

	Type	Name	Status
 	Software	Office 365	N/A
 	System/Equipment	Exchange Server	N/A
 	Third-Party Service	Tandem (Information Security Software)	Active

[+ Association](#)

- Create Asset for Business Applications
- Associate Multiple Items
- Shows in Downloads
- Can Impact CIA Ratings



15



Departmental Risk Assessments

MANY BIRDS, ONE STONE

16

Departmental Risk Assessments

DEPARTMENTAL RISK ASSESSMENTS

- Products & Services Used by Department
- Threats Affecting Day-to-Day Operations
- Similar to Business Applications



17

Threats & Controls for Departments

DEPARTMENTAL RISK ASSESSMENTS

- | | |
|--|--|
| <ul style="list-style-type: none"> • Threats <ul style="list-style-type: none"> • Loss of Key People • Operator / User Error • Unauthorized Access Due to Not Signing Out • Employee Sabotage | <ul style="list-style-type: none"> • Controls <ul style="list-style-type: none"> • Crosstraining • Employee Training • Force Automatic Logoff • Employee Termination Procedures |
|--|--|



18

Data Classifications & Data Types



DEPARTMENTAL RISK ASSESSMENTS

Public

"Data should be classified as Public when the unauthorized disclosure, alteration or unavailability of the data would result in little or no risk to the bank or its customers. Examples of Public data include marketing material, press releases, etc."

Private

"Data should be classified as Private when the unauthorized disclosure, alteration or unavailability of the data could result in a moderate level of risk to the bank or its customers. By default, all data should be considered Private unless otherwise classified."

Restricted

"Data should be classified as Restricted when the unauthorized disclosure, alteration or unavailability of the data could cause a significant level of risk to the bank or its customers. Examples of Restricted data include data protected by state or federal privacy regulations, data protected by contracts or agreements, etc."

19



Create Your Own "Template"

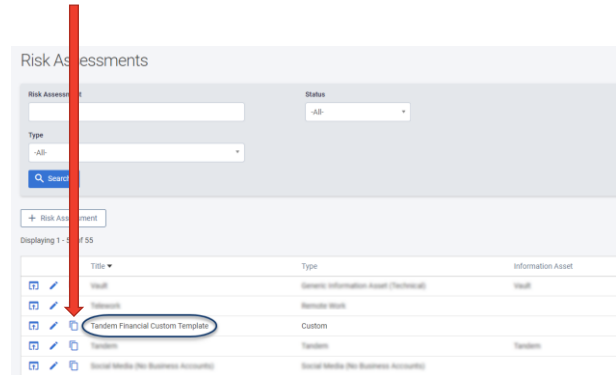
MANY BIRDS, ONE STONE

20

How do I make my own “template”?

CREATE YOUR OWN TEMPLATE

- Create Risk Assessment
- Choose Threats, Controls
- Make a “Copy” of that Risk Assessment
- Associate “Asset”
- Rinse & Repeat!



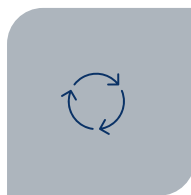
21

Many Birds, One Stone

RECAP



Assets =
Multi-Use
Tool



Suggested
Threats &
Controls



Document
Additional
Information



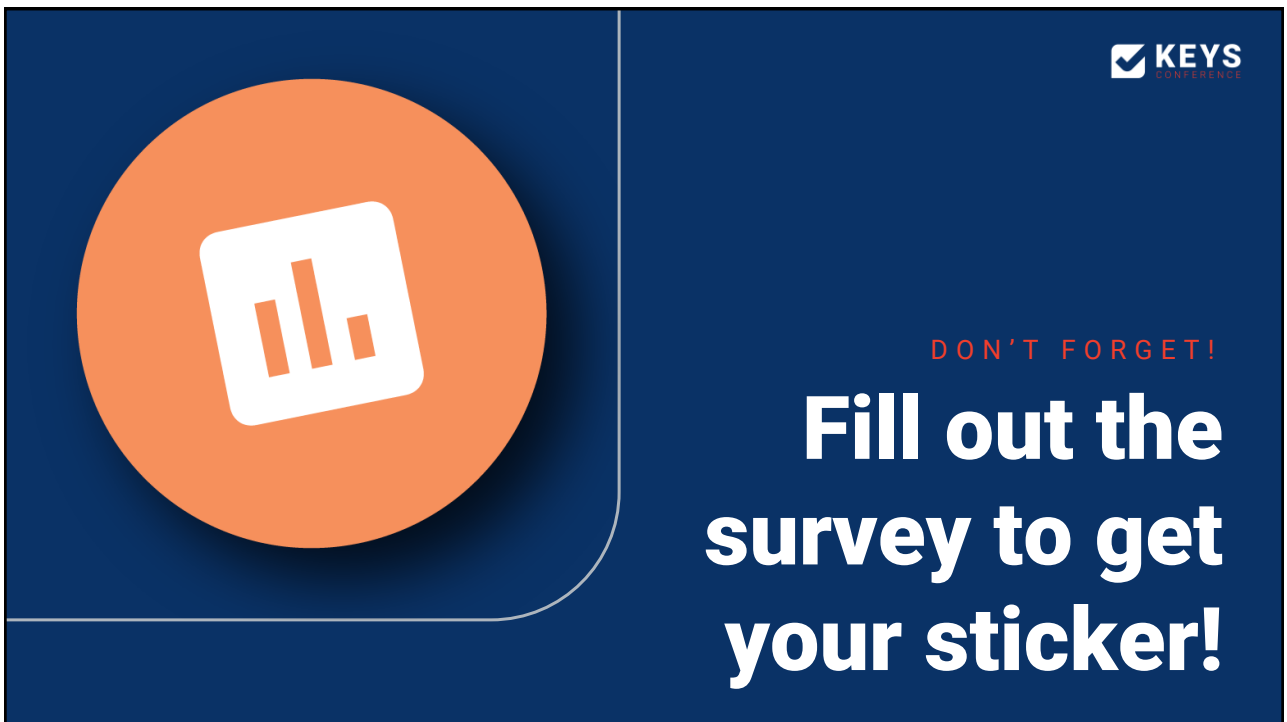
Create Your
Own
Template



22



23



24



KEYS
CONFERENCE

THANKS FOR JOINING!

**Many Birds, One Stone:
Using Asset-Based Risk
Assessments for More Than
Your Assets**

Samantha Torrez

CSXF, SOFTWARE SPECIALIST

25

Upcoming Sessions

TANDEM

So You're an Admin...

Cory Faust, Tandem

RISK & COMPLIANCE

CoNetrix Technology Engineers: A Panel Discussion

Rob Garrison, Brad Copeland, & Mike Richline, CoNetrix Technology

CYBERSECURITY

**Better Your Communication Between Technical &
Non-Technical People**

Brad Landis & Brian Whipple, Tandem



26