

Alexandria Fontana & Samantha Torrez

Tandem Risk Assessment Pre- Conference

TANDEM



1

Pre-Conference Agenda

TANDEM RISK ASSESSMENT PRECONFERENCE

- **8:30 AM - 10:00 AM:** Information Security Risk Assessment
- **10:15 AM – 11:30 AM:** Internet Banking Risk Assessments
- **11:30 AM – 12:30 AM:** Break
- **12:30 PM – 2:00 PM:** Information Asset Risk Assessments

Full agenda can be seen at <https://go.tandem.app/keys/>



2

SAMANTHA TORREZ

Information Security Risk Assessment with Tandem



3

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.



4



Samantha Torrez

TANDEM SOFTWARE SPECIALIST
CSXF



5

Agenda

INFORMATION SECURITY RISK ASSESSMENT

- What is the Information Security Risk Assessment?
- Answering the Questionnaire
- Documenting Location Information
- Reviewing Questionnaire Results
- Reviewing Threats
- Creating Risk Management Plans



6



What is the Information Security Risk Assessment?

INFORMATION SECURITY RISK ASSESSMENT

7

...” designed to identify threats that could result in the unauthorized disclosure, misuse, alteration, or destruction of financial institution or customer sensitive data.”

What is the Information Security Risk Assessment?



8

History of the ISRA

WHAT IS THE INFORMATION SECURITY RISK ASSESSMENT?

Each Financial Institution Shall:

- Identify reasonably foreseeable threats
- Assess the likelihood and potential damage of threats
- Assess the sufficiency of controls



Gramm-Leach-Bliley Act (1999)
 Interagency Guidelines Establishing Information Security Standards (2001)
 FDIC 12 CFR Part 364 Appendix B III B (Assess Risk)
 OCC 12 CFR Part 30 Appendix B III B (Assess Risk)
 NCUA 12 CFR Part 748 Appendix A III B (Assess Risk)
 FRB 12 CFR Part 208 Appendix D-2 III B (Assess Risk)



Information Security Program

WHAT IS THE INFORMATION SECURITY RISK ASSESSMENT?





Answering the Questionnaire

INFORMATION SECURITY RISK ASSESSMENT

11

Why is the questionnaire important?

ANSWERING THE QUESTIONNAIRE

Factors in Your Security Practices & Size

1

2

Provides Objective Viewpoint

Suggests Residual Risk

3



12

What's in the questionnaire?

ANSWERING THE QUESTIONNAIRE

Section	Completed
Structure and Responsibility	4/4
Size and Complexity	9/9
General Controls - 1	20/20
General Controls - 2	19/19
General Controls - 3	25/25
Previous Experience - 1	19/19
Previous Experience - 2	18/18
Natural Disaster/Elemental	14/14
Contractual, Legal and Regulatory	8/8
Audit and Security Testing	11/11
Security Awareness Training	6/6

- Asset Size
- Password Complexity / MFA Rules
- Employee Training
- Remote Deposit Capture Procedures
- DDoS Response
- Supply Chain Tracking



13

Why should I use the questionnaire?

ANSWERING THE QUESTIONNAIRE

1

Starting
Point

2

Additional
Threats

3

Easily
Updated

4

Suggested
Residual Risk



14



Location Information

INFORMATION SECURITY RISK ASSESSMENT

15

What is the purpose of Locations?

LOCATION INFORMATION

- Hazard Reporting
- Threat Recommendations
- Threat Options
- Data Pulled for Critical Locations



16

What are some other Location type threats?

LOCATION INFORMATION

Crime Threat: Fraud

Fraud

The table below lists the answers and their effect on the levels for this threat.

^ = Increase and v = Decrease

Question / Crime Data / Storm Data	Answer	Likelihood	Potential Damage
How many employees does the bank have?	1-49	^	^
What is the bank's total assets (in millions)?	\$100-\$500	^	^
In the last 12 months, has the bank experienced any unauthorized manipulation of hardware, software, or information with the intent of financial gain for the perpetrator?	No	v	
Does the bank use anti-fraud software?	Yes	v	v
Average burglaries per year	0.016735	^	^
Average larceny-thefts per year	0.052789	^	^

Storm Threat: Snow/Ice Storm

Snow / Ice Storm

The table below lists the answers and their effect on the levels for this threat.

^ = Increase and v = Decrease

Question / Crime Data / Storm Data	Answer	Likelihood	Potential Damage
Average snow/ice storms per year	3.2	^	



17

Where is this data pulled from?

LOCATION INFORMATION

- Federal Bureau of Investigation (FBI)
- National Oceanic and Atmospheric Administration (NOAA)
- Data Referenced for the Previous Year
- Annually Updated in Tandem November – December
- Not All Locations Provide Information

[Storm and Crime Statistics in Tandem](#)



18



Tandem Break!

INFORMATION SECURITY RISK ASSESSMENT

19



Reviewing Questionnaire Results

INFORMATION SECURITY RISK ASSESSMENT

20

Why do I need to review the results?

REVIEWING QUESTIONNAIRE RESULTS

Shows Residual Risk

- Current Level
- Suggested Level

First Glance at Threats

- 65 Proposed Threats

Make Changes Easily

- Update Questionnaire Answers
- Edit Threats

21

How do I review the results?

REVIEWING QUESTIONNAIRE RESULTS

Fire

The table below lists the answers and their effect on the levels for this threat.
 ^ = Increase and v = Decrease

Question / Crime Data / Storm Data	Answer	Likelihood	Potential Damage
How many locations does the bank have?	6-25	^	^
Regarding fire detection and prevention, select all that apply:	The bank has a fire suppression system (e.g., fire sprinklers, etc.)	v	v
Regarding fire detection and prevention, select all that apply:	The bank has fire extinguishers.		v
Regarding fire detection and prevention, select all that apply:	Inspection of fire extinguishers are current.		v
Is it reasonable to believe the backup media location would be susceptible to disruption by the same natural disaster event (e.g., tornado, hurricane, fire, etc.) as the data center?	No		v
Average wild and forest fires per year	0.909090909	^	^
Average arson related crimes per year	0.000401	^	^

Look for:

- The Question(s) / Crime Data / Storm Data affecting the threat
- If the answer / data increased or decreased the Likelihood and Potential Damage

22

How Questions & Stats Work Together

REVIEWING QUESTIONNAIRE RESULTS

- More branches = higher likelihood & higher risk
- Fire prevention practices reduce risk
 - Fire Suppression System
 - Fire Extinguishers
 - Inspection
- Backup data at separate location
- Wildfires / Forest Fires
- Arson

Fire

The table below lists the answers and their effect on the levels for this threat.
 ^ = Increase and v = Decrease

Question / Crime Data / Storm Data	Answer	Likelihood	Potential Damage
How many locations does the bank have?	6-25	^	^
Regarding fire detection and prevention, select all that apply: The bank has a fire suppression system (e.g., fire sprinklers, etc.)		v	v
Regarding fire detection and prevention, select all that apply: The bank has fire extinguishers.			v
Regarding fire detection and prevention, select all that apply: Inspection of fire extinguishers are current.			v
Is it reasonable to believe the backup media location would be susceptible to disruption by the same natural disaster event (e.g., tornado, hurricane, fire, etc.) as the data center?	No		v
Average wild and forest fires per year	0.909090909	^	^
Average arson related crimes per year	0.000401	^	^



23

Approving Suggested Residual Risk

REVIEWING QUESTIONNAIRE RESULTS

	Suggested Level	Low	Moderate	Medium	
Exploitation by Cyber Attack	Current Level	Low	Moderate	Low	
	Suggested Level	Low	Moderate	Medium (Approve)	
Faulty Password System	Current Level	Low	Moderate	Medium	
	Suggested Level	Medium (Approve)	Major (Approve)	High (Approve)	
Faulty Termination Procedures	Current Level	Medium	Minimal	Low	



24



Tandem Break!

INFORMATION SECURITY RISK ASSESSMENT

25



Reviewing Threats

INFORMATION SECURITY RISK ASSESSMENT

26

Where should I start?

REVIEWING THREATS

- Enable Inherent Risk
- Sort by Residual Risk
- Use Included Filter
- Start with Familiarity

Information Security - Threats

included
-All-
Search

+ Threat

Displaying 1 - 65 of 65

Name	Included	Inherent Risk	Residual Risk	Risk Management Plan	Description
Electronic Banking System Misuse	Yes	TBD	High	Accept	Proposed Threat
Faulty Password System	Yes	TBD	High	Accept	Proposed Threat
Data on Removable Media Compromised	Yes	TBD	Medium	Accept	Proposed Threat
Employee Sabotage	Yes	TBD	Medium	Accept	Proposed Threat
Fire	Yes	TBD	Medium	Accept	Proposed Threat
ATM System Compromised	Yes	TBD	Low	Accept	Proposed Threat



27

What should I be reviewing in my threats?

REVIEWING THREATS



Title, Details,
and Included



Threat
Category &
Threat Type



Inherent Risk



Controls &
Residual Risk



28

REVIEWING THREATS

In the ISRA, adjusting controls will not automatically adjust your residual risk.

When you adjust controls, be sure to also adjust your risk.



29

Why are policies suggested as controls?

REVIEWING THREATS

1

High Level
Risk Assessment

2

Define Control
Environment

3

Your Practices
Impact Risk

FFIEC Information Security Booklet, II.C.1 – Policies, Standards, and Procedures



30

Why are policies suggested as controls?

REVIEWING THREATS

“Policies, standards, and procedures should define the institution's control environment through a governance structure and provide descriptions of required, expected, and prohibited activities”

FFIEC Information Security Booklet, II.C.1 – Policies, Standards, and Procedures



31

What should I be reviewing in my threats?

REVIEWING THREATS



Title, Details,
and Included



Threat
Category &
Threat Type



Inherent Risk



Controls &
Residual Risk



Verifications
& Potential
Impacts



32



Tandem Break!

INFORMATION SECURITY RISK ASSESSMENT

33



Creating Risk Management Plans

INFORMATION SECURITY RISK ASSESSMENT

34

Why do I need risk management plans?

CREATING RISK MANAGEMENT PLANS



Provides Explanation



Proof for Audits / Exams



35

How do I choose a Risk Management Plan?

CREATING RISK MANAGEMENT PLANS

Accept

**Mitigate
Further**

Transfer

Defer



36

What should be included in my RMP?

CREATING RISK MANAGEMENT PLANS

- Recommended when choosing anything other than “Accept”
 - Details can still be listed for “Accept”
- Additional Mitigation Plans
- Control Details
- Options for Transferring & Deferring Risk



37

CREATING RISK MANAGEMENT PLANS

Your risk management plans should cover how you plan to handle the risks your institution faces.



38

Tandem Break!

INFORMATION SECURITY RISK ASSESSMENT

39

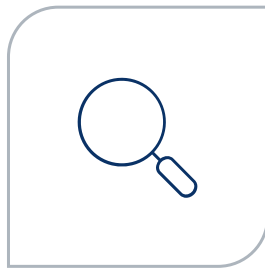
Summary

INFORMATION SECURITY RISK ASSESSMENT

Questionnaire & Locations Provide Residual Risk



Reviewing Threats & Make Changes



Review Questionnaire to See Suggestions



Create Risk Management Plans to Track Risk

40



You have completed the Information Security Risk Assessment!

TANDEM RISK ASSESSMENT



41



42

ALEXANDRIA FONTANA

Internet Banking Risk Assessments with Tandem



43



Alexandria Fontana

TANDEM SOFTWARE SPECIALIST
CSXF



44

Agenda

INTERNET BANKING RISK ASSESSMENTS

- Questionnaires
- Internet Banking Risk Assessment Examples
- Customer Education
- Tandem's Response to FFIEC Updates (Authentication & Access Guidance)



45



Internet Banking Admin Questionnaire

INTERNET BANKING RISK ASSESSMENTS

46

What's the focus of this questionnaire?

INTERNET BANKING ADMIN QUESTIONNAIRE

- Organization Size & Complexity
- Internal Controls
 - Segregation of E-Banking Duties
 - Social Engineering Training
 - Backup Media Encryption
- Vendor Management
 - Reviewing Internet Banking Vendors
- Previous Experience
 - Internet Banking Misuse Experience
- Audit and Security Testing
 - Audits, Vulnerability Assessments, Social Engineering Tests



47

What the Questionnaire Does

INTERNET BANKING ADMIN QUESTIONNAIRE

Fraud ×

The table below lists the answers and their effect on the levels for this threat
 ▲ = Increase and ▼ = Decrease

Question	Answer	Likelihood	Potential Damage
How many internet banking customers (specific to the type of this risk assessment) does the bank have?	Over 500	▲	▲
What services are offered to internet banking users, specific to the type of this risk assessment? (Select all that apply)	Accessing/viewing account information	▲	▲
Does the bank have fraud detection controls that would prompt for additional review and reporting of suspicious activities involving internet banking?	Yes	▼	▼
Does the bank's customer awareness and education program include a suggestion that commercial online banking customers periodically perform a related risk assessment and controls evaluation?	Yes	▼	▼
What services are offered to internet banking users, specific to the type of this risk assessment? (Select all that apply)	Bill payment	▲	▲
What services are offered to internet banking users, specific to the type of this risk assessment? (Select all that apply)	Intrabank funds transfers	▲	▲
How would you best describe the largest dollar amount possible for an internet banking transaction (specific to the account type(s) covered in this risk assessment)?	High	▲	▲
Are maximum transaction dollar limits in place?	Yes	▼	▼
In the last 12 months, has the bank detected internet banking fraud from their customers?	Yes	▲	▲
Are limits in place to restrict transaction volume?	Yes	▼	▼

Review Questionnaire Results

- Which answers increased my residual risk?
- Which answers decreased my residual risk?
- What is the overall residual risk?



48

Threats - Internet Banking Admin

INTERNET BANKING ADMIN QUESTIONNAIRE



Exploitation by
Cyber Attack



Inadequate Vendor
Management



Software Problem
or Failure



Vishing



49

Controls for Internet Banking Admin

INTERNET BANKING ADMIN QUESTIONNAIRE

- Mostly “Policies” as Controls
- Controls Used:
 - Acceptable Use of Information Assets Policy
 - Employee Security Awareness Training Policy
 - Intrusion Detection / Prevention System
 - Vulnerability and Patch Management Policy

**Training Your
Employees with
Tandem**

THURSDAY
9:10 AM
TANDEM TRACK



50



Internet Banking Customer Questionnaire

INTERNET BANKING RISK ASSESSMENTS

51

What's the focus of this questionnaire?

INTERNET BANKING CUSTOMER QUESTIONNAIRE

- Organization Size & Complexity
- Authentication Controls
 - Methods Used to Authenticate Users
 - Challenge Questions
- General Controls
 - Transaction Limits
 - Review of Transactions
- Customer Awareness and Education
- Previous Experience
- Contractual, Legal, and Regulatory
- Audit and Security Testing



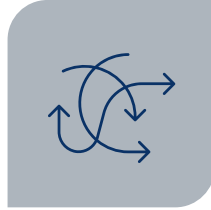
52

Threats - Internet Banking Customer

INTERNET BANKING CUSTOMER QUESTIONNAIRE



Man-in-the-Browser
(MIB) Attack



Pharming



SMSishing
(SMS Phishing)



Website
Spoofing



53

Controls for Internet Banking Customer

INTERNET BANKING CUSTOMER QUESTIONNAIRE

- Customer Awareness and Education
- Day / Time Restrictions
- Multi-Factor Authentication
- User Session Timeout

POP QUIZ

**What is
Tandem's user
session timeout?**



54



Tandem Break!

INTERNET BANKING SECURITY PROGRAM

55



Internet Banking Risk Assessment Examples

INTERNET BANKING RISK ASSESSMENTS

56

When do I use these questionnaires?

INTERNET BANKING RISK ASSESSMENT EXAMPLES

Internet Banking Admin

1

2

Commercial Internet Banking

Retail Internet Banking

3



57

What is commercial internet banking?

INTERNET BANKING RISK ASSESSMENT EXAMPLES

“Electronic payment system that enables business banking customers to conduct a range of financial transactions through the website by connecting to a core banking system”

<https://www.lawinsider.com/dictionary/corporate-internet-banking>
<https://www.investopedia.com/terms/b/business-banking>



58

What is retail internet banking?

INTERNET BANKING RISK ASSESSMENT EXAMPLES

“Banking that provides financial services to individual consumers rather than businesses”

<https://www.investopedia.com/terms/r/retailbanking>
<https://www.investopedia.com/terms/b/business-banking>



59

INTERNET BANKING RISK ASSESSMENT EXAMPLES

Answer the questions based on what you're assessing – either retail or commercial services.



60



Customer Education

INTERNET BANKING RISK ASSESSMENTS

61

WHY DO I NEED CUSTOMER EDUCATION?

**Recommended by
FFIEC Supplement to
Authentication in an
Internet Banking
Environment Booklet**



62

Education should...

CUSTOMER EDUCATION

Explanation of protections provided & not provided

Explains

List of alternative control mechanisms customers could implement

Controls

Suggestions

Suggestion for the customer to do self-risk assessment & controls evaluation

Conditions

When the institution may contact the customer

Contacts

List of institutional contacts to report suspicious activity to



63

What are the customer education options?

CUSTOMER EDUCATION



Online Banking Security Tips



Avoiding Social Engineering Attacks



Mobile Financial Services



Self-Risk Assessments



64

Online Banking Security Tips

CUSTOMER EDUCATION

- **Mobile Device Security**
 - Require Passcode
 - Keep software up-to-date
 - Sign-out of apps
- **Online Security**
 - Don't click suspicious / unknown links
 - Website Encryption
 - Don't use public devices
- **General PC Security**
 - Up-to-date antivirus
 - Utilize Firewalls
 - Require Password
- **Passwords**
 - Different Passwords for Different Accounts
 - Long Passwords
 - Avoid using common information



65

THE RISK ASSESSMENT & CONTROL EVALUATION

Intended to “help commercial internet banking users identify threats and measure the strength of their controls”.



66

The Risk Assessment & Control Evaluation

- Questions about:
 - Personnel Security
 - System Security
 - Physical Security
 - Previous Experience



67



Tandem Break!

INTERNET BANKING SECURITY PROGRAM

68



Tandem's Response to FFIEC Updates

Internet Banking Risk Assessments

69

What FFIEC Updates?

TANDEM'S RESPONSE TO FFIEC UPDATES

FFIEC Authentication and Access to Financial Institution Services and Systems Guidance

- Replaces previous documentation (2005 & 2011)
- Current Cybersecurity Threat Environment; Increased Remote Access
- Importance of risk assessments for authentication practices
- Emphasis layered security; importance of MFA
- Examples of Authentication Controls

<https://www.ffiec.gov/press/pr081121.htm>



70

How will Tandem Respond?

TANDEM'S RESPONSE TO FFIEC UPDATES



Questionnaires



Threats



Controls



Document Introductions



Customer Education Resources



New Terminology & Considerations from Guidance



71

Summary

INTERNET BANKING SECURITY PROGRAM



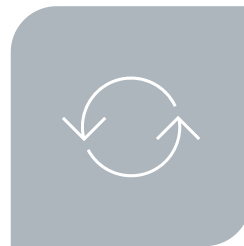
Questionnaires Provide Residual Risk



Associate Assets to Provide Additional Details



Customer Education Provided by Tandem



Updates from the FFIEC Guidance



72



You have completed the Internet Banking Risk Assessments!

TANDEM INTERNET BANKING SECURITY PROGRAM



73



74

Samantha Torrez

Asset-Based Risk Assessments with Tandem



75

Agenda

ASSET-BASED RISK ASSESSMENTS

- Difference Between Asset Based vs Questionnaire Based
- Managing Information Assets
 - Data Classifications & Data Types
- Importance of Associations, Custom Fields, and Security Requirements
- Risk Assessment Types
- Applying Threats & Controls
- Integrations with other Tandem Products



76

Difference Between Asset & Questionnaire Based Assessments

Asset-Based Risk Assessments

77

What's the difference?

DIFFERENCE BETWEEN ASSET BASED & QUESTIONNAIRE ASSESSMENTS

Questionnaire Based:

- Use Questionnaires
- No Risk Assessment Types
- Risk based off Questionnaire & Location Results
- High-Level Overview of Risk
- Policies
- No Control Reduction Values

Asset Based:

- No Questionnaire
- Use Risk Assessment Types
- Risk based off Assets / RA Type
- Specific Threats & Controls Applied
- Controls
- Control Reduction Values Applied

78

“Why do I need both?”

The asset management tool can help you determine the importance of your institution's assets, and which warrant risk assessments.

79

Managing Information Assets

Asset-Based Risk Assessments

80

MANAGING INFORMATION ASSETS

An information asset is anything that accesses, stores, transmits, or protects information.



81

Examples of Information Assets

MANAGING INFORMATION ASSETS



ACH System



Employees



Mobile Devices



Remote Work



Wire Transfer System



82

FFIEC AIO BOOKLET:

“Data identification and data classification are important components of data management. To effectively manage data, it is important to identify what data the entity has, particularly to identify sensitive customer and entity information.”



83

Data Classifications



MANAGING INFORMATION ASSETS

Public

“Data types should be classified as “Public” when the unauthorized disclosure, alteration, or unavailability of the data would result in little or no risk to the institution or its customers.”

Private

“Data types 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 institution or its customers. By default, all data types should be considered “Private,” unless otherwise classified.”

Restricted

“Data types should be classified as “Restricted” when the unauthorized disclosure, alteration, or unavailability of the data could cause a significant level of risk to the institution or its customers.”

84

Data Types

MANAGING INFORMATION ASSETS

- ACH Origination (Restricted)
- Backup Files (Restricted)
- Contact Information (Public)
- Employee Applications (Private)
- Loan Files (Restricted)
- Wire Transfer Information (Restricted)



85



Tandem Break!

ASSET-BASED RISK ASSESSMENTS

86

Associations, Custom Fields, and Security Requirements

Asset-Based Risk Assessments

87

When should I use Associations?

ASSOCIATIONS, CUSTOM FIELDS, AND SECURITY REQUIREMENTS



Use Associations to show if the asset contains data that is needed by your organization for business continuity purposes.



These associations should impact your asset's "Availability" rating

88

Association Examples

ASSOCIATIONS, CUSTOM FIELDS, AND SECURITY RATINGS

Software

1

2

Systems/Equipment

Third Parties

3



89

Custom Fields

ASSOCIATIONS, CUSTOM FIELDS, AND SECURITY REQUIREMENTS



Checkbox



Date



Dropdown
(One or
Multiple)



Integer



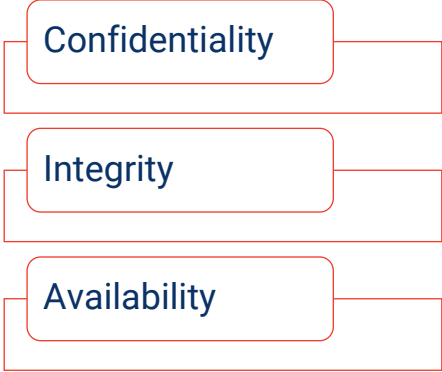
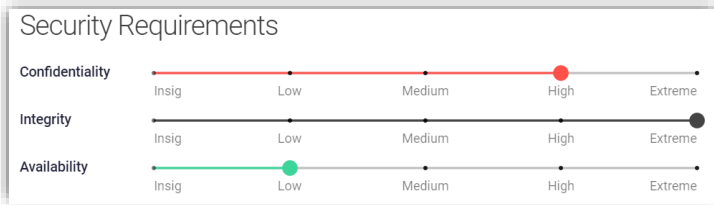
Plain Text
or Rich
Text



90

Security Requirements

ASSOCIATIONS, CUSTOM FIELDS, AND SECURITY REQUIREMENTS



91

Why are Security Requirements important?

ASSOCIATIONS, CUSTOM FIELDS, AND SECURITY REQUIREMENTS

Security Requirements			
Confidentiality	Integrity	Availability	CIA Rating ©
● High	● Extreme	● High	● 84
● Medium	● Extreme	● Medium	● 65
● High	● Extreme	● Low	● 65
● Extreme	● Extreme	● Extreme	● 95
● High	● High	● High	● 78
● High	● Medium	● Medium	● 59
● High	● High	● Medium	● 68

- Security Requirements rate the importance of your assets.
- At a minimum, do risk assessments over assets with a CIA rating over 75.



92

Why are Security Requirements important?

ASSOCIATIONS, CUSTOM FIELDS, AND SECURITY REQUIREMENTS

Information Asset	CIA Rating	Residual Risk Overview			Overall Risk
Backup System	95	2	12	9	High
Accounting System	84	2	12	8	High
Telework	84	12		16	Medium
Firewall / Perimeter Devices	83	5	6		High
Mobile Application	80	4	11		Medium
Core Processing	78	3	15	4	Medium

- Security Requirements rate the importance of your assets.
- At a minimum, do risk assessments over assets with a CIA rating over 75.



Tandem Break!

ASSET-BASED RISK ASSESSMENTS

Risk Assessment Types

Asset-Based Risk Assessments

95

What are Risk Assessment Types?

RISK ASSESSMENT TYPES



“Risk Assessment Types are templates that provide an initial list of threats and controls based on the asset for which they were designed.”



Risk Assessment > Assets > Risk Assessment > “+”

Risk Assessment

Create a New Risk Assessment

Click the Continue button below to create a new risk assessment for this information asset and open the risk assessment.

Note: The new risk assessment will be named the same as this asset.

Risk Assessment Type*

Generic Information Asset (Technical) ▾

+ Continue

96

Risk Assessment Type Options

RISK ASSESSMENT TYPES

ACH System

ATM

Cloud Computing

Custom

Generic Information Asset (Technical)

Mobile Devices

Mobile Financial Services

Prepaid Cards

RDC – Merchant & Consumer

RDC – Mobile Capture

Remote Work

Social Media

Social Media (No Business Accounts)

Tandem

Wire Transfer System



97

What are other options for creating ABRA's?

RISK ASSESSMENT TYPES

1

Custom Type

2

Select Existing

3

Copy Existing



98



Tandem Break!

ASSET-BASED RISK ASSESSMENTS

99



Applying Threats & Controls

Asset-Based Risk Assessments

100

Reviewing Threats

APPLYING THREATS & CONTROLS

Exclude Unnecessary Threats*

1

2

Add Custom Threats

Review Descriptions

3



*Tandem Suggested threats cannot be deleted.

101

What's in these threats?

APPLYING THREATS & CONTROLS



Title, Details,
and Included



Threat Type



Inherent Risk
& Residual
Risk



Controls



Risk
Management
Plan

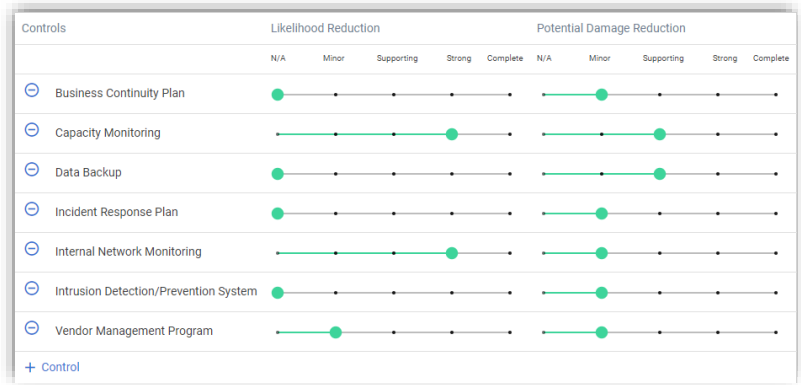


102

What's different about Controls?

APPLYING THREATS & CONTROLS

- How much does this control **reduce the likelihood** of this threat from happening?
- How much does this control **reduce the potential damage** this threat could cause?

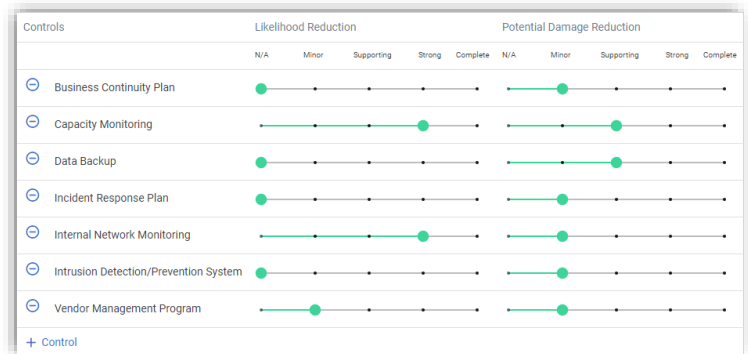


103

What are Control Reduction Values?

APPLYING THREATS & CONTROLS

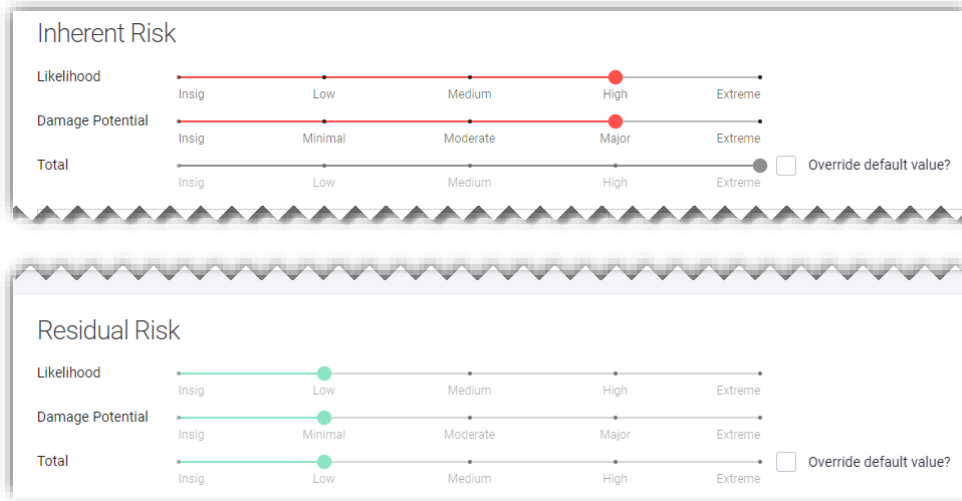
- **N/A:** No effect on reducing risk.
- **Minor:** Can slightly reduce risk.
- **Supporting:** Supports other controls to reduce risk.
- **Strong:** Can greatly reduce risk.
- **Complete:** Practically eliminates the risk on its own.



104

Inherent to Residual Risk

APPLYING THREATS & CONTROLS

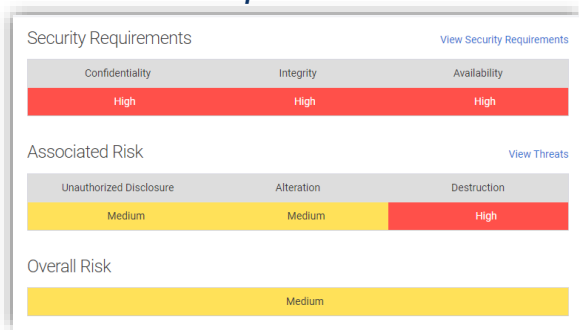


105

Overall Risk Calculation

APPLYING THREATS & CONTROLS

Risk Assessment > Open RA > Dashboard



CIA & Threat Types* Associations:

- Unauthorized Disclosure = Confidentiality
- Alteration = Integrity
- Destruction = Availability

[Asset Management: Overall Risk Calculation](#)

*Note: Misuse is not included as part of this calculation.



106

APPLYING THREATS & CONTROLS

Don't forget your Risk Management Plans in your Asset-Based Risk Assessments!



107



Tandem Break!

ASSET-BASED RISK ASSESSMENTS

108



Integrations

Asset-Based Risk Assessments

109

Tandem Risk Assessment Integrations

INTEGRATIONS



Audit Management Standard & Pro



Business Continuity Plan



Incident Management



Policies



Social Media Management



Vendor Management



110

Audit Management

INTEGRATIONS

Audit Management Standard:

- Allows organizations to create individual “containers” for their testing results.
- Document Findings
- Track Responses
- Associate Controls

Audit Management Pro:

- Allows organizations to create control verifications and organize their testing procedures into work programs.
- Create Control Evidence & Request List Items
- Document Findings
- Associate Controls



111

How do I enable this integration?

INTEGRATIONS

Risk Assessment:

Core Processing - Settings

General Settings Information Asset

Audit

Enable Audit Association ⓘ

Guidance

Add guidance from standards and regulations that helps define threats and/or mitigation strategies for this assessment. Additional guidance can be added to the master list through the **Guidance** settings page.

Guidance
12 CFR Part 364 Appendix B (Interagency Guidelines Establishing Information Security Standards)
FFIEC IT Examination Handbook, Information Security Booklet
Gramm-Leach-Bliley Act, Title V, Subtitle A, Section 501(b)

+ Guidance

Save

Audit Management:

Edit 2022 (Auditee) IT/GLBA Audit

Audit Details Access Groups Custom Levels Audit Ratings **Advanced Options**

Verification ⓘ

Residual Risk ⓘ

Approval ⓘ

Risk Assessment Association ⓘ



112

How does this work on the ABRA side?

INTEGRATIONS

Asset-Based Risk Assessment



113

How does this work on the Audit side?

INTEGRATIONS

Open Audit > Controls

Control ▲	Status	Finding
<input checked="" type="checkbox"/> Anti-Malware Software	● Pass	
<input checked="" type="checkbox"/> Employee Security Awareness Training	● Fail	The organization's employee security awareness training over remote access is inadequate.
<input checked="" type="checkbox"/> Firewall	● Pass	
<input checked="" type="checkbox"/> Limit Local Administrator Access	● Pass	
<input checked="" type="checkbox"/> Patch Management	● Pass	





114

How does this work on the Audit side?

INTEGRATIONS



Open Audit > Controls

Findings ⓘ

Finding	
 	ITGLBA.22 Annual SAT has not been updated since 2019.

+ Finding + Previous Finding

Risk Assessment Controls

Control	
 	Employee Security Awareness Training

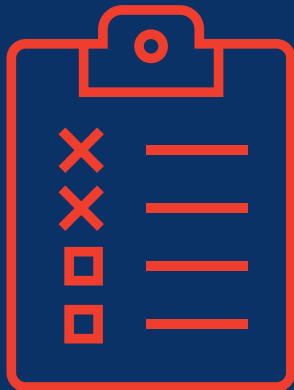
+ Control



115

What should I do if a control fails testing?

INTEGRATIONS



- Why did the control fail?
- What solutions can we use to get it to pass?
- Do we need to accept the risk of this control and invest in compensating / mitigating controls?



116

BCP & Vendor Management

INTEGRATIONS

- Associate Software, Systems/Equipment, Third-Party Services
- Shows Related Business Process & Vendor Service Info

Business Processes

Business Process	Criticality	Maximum Tolerable Downtime (MTD) ⓘ
Account Reconciliation	● Important	3 Days
Automated Clearing House (ACH)	● Critical	2 Hours
Email Processing	● Urgent	24 Hours

Vendor Services ⓘ

Vendor (Service)	Significance	Overall Risk	Status
FiServ (Core Processing)	● Critical	● High	Active



117

Vendor Management Perspective

INTEGRATIONS

Edit Vendor Service

Service *
Core Processing

Status *
Active

Profile Significance Risk Assessment Responsibility Locations

Risk Assessment

Overall Risk ⓘ

Comments (0) Definitions

Information Asset Associations ⓘ

Asset	Status	Confidentiality	Integrity	Availability	Overall Risk
Backup System	Active	● Extreme	● Extreme	● Extreme	● High
Accounting System	Active	● High	● Extreme	● High	● High

+ Association

- Associate Asset within Vendor Service > Risk Assessment
- Displays:
 - Asset Status
 - CIA Information
 - Overall Risk



118

Incident Management

INTEGRATIONS

☰ Risk Assessment

General Assets ACH System × + Open

- Dashboard
- Controls
- Threats
- Incidents**
- Reports
- Revision/Approval Log
- Download Documents

Incidents

Displaying 1 - 1 of 1

ID	Name	Severity
1010-CRIME	Customer ACH Fraud Attempt	Medium



119

Incident Management

INTEGRATIONS

Analysis ⓘ

Associations

Business Processes Affected

+ Add System/Equipment

Information Assets Affected

Information Asset	CIA Rating ⓘ
ACH System	65

+ Add Information Asset



120

Policies

INTEGRATIONS

Information S

These are the policies and c controls will be assigned to proposed threats where app take advantage of the defau

Included Not Included

Controls referenced by at le

Displaying 1 - 53 of 53

Title ▲

- Acceptable Use of
- Access Control Po
- Administrators Pol
- Asset Managemer
- ATM Security Pol

Controls ⓘ

Control
Acceptable Use of Information Assets Policy
Access Control Policy
Employee Security Awareness Training Policy
Incident Management Policy
Mobile Devices Policy
Remote Work Policy
Removable Media and Data Transfer Policy
Reporting of Security Violations Policy
Security Testing Policy

hese
to the
your own to



121

What does this look like in Policies?

INTEGRATIONS

Threats ⓘ

Threat
Exploitation by Cyber Attack
Inadequate Logical Access Controls
Inadequate Physical Access Controls
Inadequate Vendor Management
Installation of Unauthorized Software
Malicious Software
Poor Oversight of Information Technology
Software Problem / Failure
System Hardware Problem / Failure

Note: Changing these threats will also update your information security risk assessment.



122

Social Media Management

INTEGRATIONS

Risk Management Introduction

✂ 📄 📁 ↶ ↷ 🔍 🔗 🔍 🔍 🔍 🔍 🔍 🔍 🔍 🔍 🔍 🔍 🔍 🔍 🔍 🔍

The use of social media to attract and interact with customers can impact a bank's risk profile, including risk of harm to customers, compliance risks, legal risks, operational risks, and reputation risks. Increased risk can arise from poor due diligence, oversight, or control on the part of the bank. The purpose of this risk assessment is to assist Tandem Financial in identifying potential risks related to social media to ensure it has implemented adequate controls, policies, and procedures to mitigate these risks to an acceptable level.

The saved text above is the proposed text.

Risk Assessments

Type	Title	Status
	Social Media	Social Media Active

[+ Risk Assessment](#)



Social Media Threats

INTEGRATIONS

2.1 Social Media Risk Matrix

Ref	Threat	Inherent Risk	Controls	Residual Likelihood	Residual Damage Potential	Residual Risk	Risk Mgmt. Plan
5.1	BSA/AML Noncompliance	High	Approval of Social Media Content, Banking Services Not Accessible via Social Media, Customer Identification Program (CIP), Employee Training, Fraud Detection System, Monitoring Social Media/Internet, Services Not Marketed via Social Media	Low	Minimal	Low	Accept
<i>Approval of Social Media Content</i>							
5.15	FHA Noncompliance	Medium	Approval of Social Media Content, Employee Training, Monitoring Social Media/Internet, Services Not Marketed via Social Media	Insignificant	Moderate	Low	Accept
5.14	GLBA Noncompliance	Medium	Approval of Social Media Content, Banking Services Not Accessible via Social Media, Customer Awareness and Education, Employee Training, Monitoring Social Media/Internet	Insignificant	Moderate	Low	Accept
5.15	Personal Use of Bank Email	Medium	Employee Security Awareness Training, Employee Training, Monitoring Social Media/Internet, Restricting Employee Email Accounts from Social Media	Low	Minimal	Low	Accept
5.16	RESPA Noncompliance	Medium	Approval of Social Media Content, Banking Services Not Accessible via Social Media, Employee Training, Incident Response Plan, Monitoring Social Media/Internet, Services Not Marketed via Social Media	Insignificant	Moderate	Low	Accept
5.17	Spooled Social Media Account	High	Customer Awareness and Education, Employee Security Awareness Training, Incident Response Plan, Monitoring Social Media/Internet	Medium	Moderate	Medium	Mitigate Further





Tandem Break!

ASSET-BASED RISK ASSESSMENTS

125

Recap

ASSET-BASED RISK ASSESSMENTS

- Managing Assets & Documenting Additional Information
- Risk Assessment Types
- Applying Threats & Controls
- Control Reduction Values
- Using Integrations



126



127



128



DON'T FORGET!

**Please fill out
the survey!**