WELCOME TO

What the New ACET Means for Your Next IT Exam

Leticia Saiid, Security+
Chief of Staff
Tandem, LLC

Tandem

Can You Hear Me?

- We are audio broadcasting so please plug in your headphones or computer speakers to listen in.
- If your audio is choppy or slow, you may wish to dial into the teleconference:

- **Telephone:** +1 646 558 8656
  Webinar ID: 819 0414 4222
- **Passcode:** 4298845

Tandem

Slide Link

Today’s slides can be found online at:
http://bit.ly/2022-01-20-acet

Tandem

We Encourage Questions

Use the

Questions Box

located on the bottom of your screen to type your comments or questions.

Tandem™

Tell Us What You Think!

Please take our post-event survey. We value your feedback!

Tandem

Disclaimer

- **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.

Tandem

Tandem™

A CoNetrix company

PRESENTER

Leticia Saiid, Security+

Chief of Staff

Tandem™

Tandem™


ME
ACET

Agenda

1. History, Definitions, Roles
2. Exam Expectations
3. ACET Application Options
4. Q & A

Tandem™

History
Definitions
Roles

Tandem™

Pop Quiz

What does the “E” stand for in ACET?

A Examination

B Expectations

C Estimation

D Evaluation

Tandem™

"The NCUA has transitioned its priority from performing **Automated Cybersecurity Examination Tool** (ACET) cybersecurity maturity assessments, to evaluating critical security controls. The NCUA is also piloting an Information Technology Risk Examination solution for Credit Unions (InTREx-CU)."

UPDATED 2020 SUPERVISORY PRIORITIES (JULY)

The agency has reprioritized away from performing facilitated **Automated Cybersecurity Evaluation Toolbox** (ACET) cybersecurity maturity assessments, to piloting the Information Technology Risk Examination for Credit Unions (InTREx-CU). […] The InTREx-CU will continue to be deployed in 2021 […] ACET will become a self-assessment resource for [CUs], supported by the NCUA.

2021 SUPERVISORY PRIORITIES (JANUARY)

Pop Quiz

What does the “E” stand for in ACET?

A Examination

B Expectations

C Estimation

D Evaluation

Tandem

I will be clear by labeling

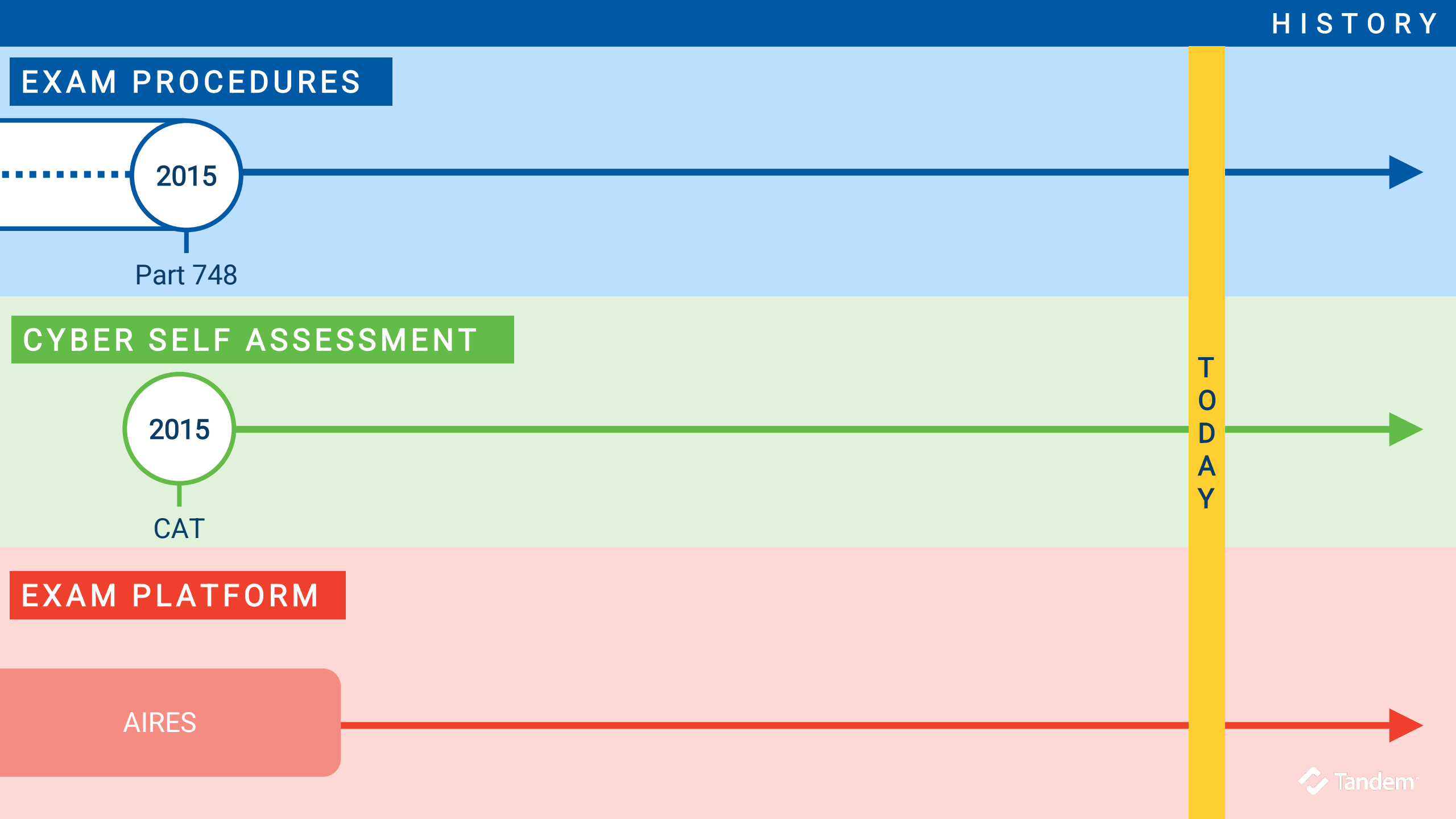
ACExT

Automated
Cybersecurity
Examination
Tool

ACEvT

Automated
Cybersecurity
Evaluation
Toolbox

Tandem™


HISTORY
EXAM PROCEDURES
2015
Part 748
CYBER SELF ASSESSMENT
2015
CAT
TODAY
EXAM PLATFORM
AIRES
Tandem

NCUA SUPERVISORY PRIORITY LETTERS

2015

"Credit unions, like all financial institutions, remain vulnerable to internal and external cybersecurity threats. Last year's interagency cybersecurity assessment conducted through the [FFIEC] found that many credit unions and banks are not taking basic cybersecurity actions."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/supervisory-priorities-2015

Tandem

National Credit Union Administration

Regulatory Reporting

CUOnline

Corporate Credit Union Online

AIRES Exam Software Information

CUSO Registry

Collection of Examination & Supervision Information

AIRES Exam Software Information

The NCUA Examiners use our Automated Integrated Regulatory Examination System (AIRES) to complete examinations. AIRES is a combination of Visual Basic and Microsoft Excel, Access and Word Programs.

AIRES Exam Questionnaires

AIRES IT Exam Questionnaires - Several optional questionnaires are available to examiners reviewing a credit union's information technology. The questionnaires focus on Information Technology, Audit, and Member Services.

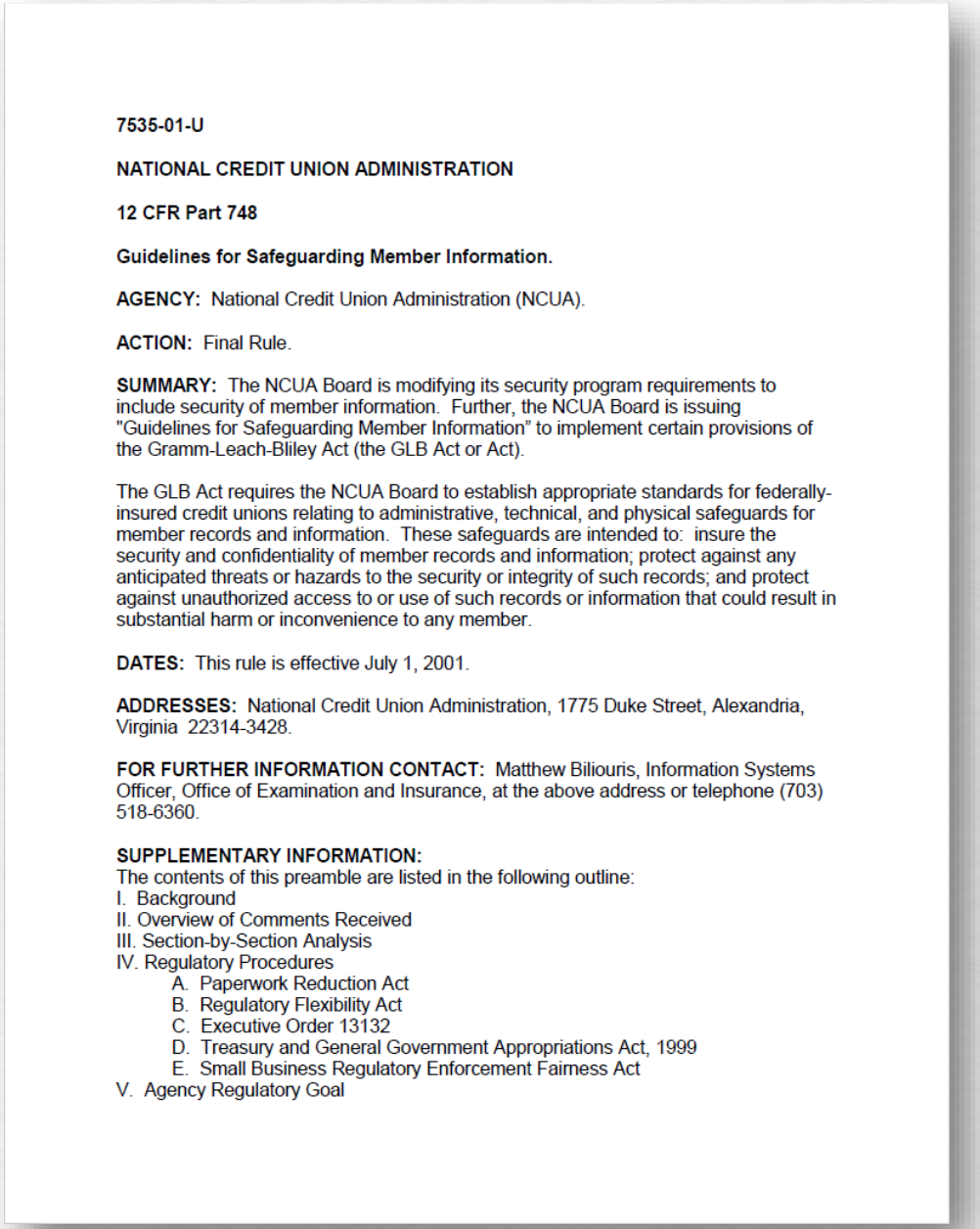
The AIRES file layout specifications are found in Letter to Credit Unions 03-CU-05.

Frequently Asked Questions for Share and Loan Record Layout

If you have any questions, please send an e-mail to the Office of Examination and Insurance (eimail@ncua.gov).

Last modified on 05/11/21

https://www.ncua.gov/regulation-supervision/regulatory-reporting/aires-exam-software-information



7535-01-U

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 748

Guidelines for Safeguarding Member Information.

AGENCY: National Credit Union Administration (NCUA).

ACTION: Final Rule.

SUMMARY: The NCUA Board is modifying its security program requirements to include security of member information. Further, the NCUA Board is issuing "Guidelines for Safeguarding Member Information" to implement certain provisions of the Gramm-Leach-Bliley Act (the GLB Act or Act).

The GLB Act requires the NCUA Board to establish appropriate standards for federally-insured credit unions relating to administrative, technical, and physical safeguards for member records and information. These safeguards are intended to: insure the security and confidentiality of member records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any member.

DATES: This rule is effective July 1, 2001.

ADDRESSES: National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314-3428.

FOR FURTHER INFORMATION CONTACT: Matthew Biliouris, Information Systems Officer, Office of Examination and Insurance, at the above address or telephone (703) 518-6360.

SUPPLEMENTARY INFORMATION:
The contents of this preamble are listed in the following outline:

I. Background
II. Overview of Comments Received
III. Section-by-Section Analysis
IV. Regulatory Procedures
    A. Paperwork Reduction Act
    B. Regulatory Flexibility Act
    C. Executive Order 13132
    D. Treasury and General Government Appropriations Act, 1999
    E. Small Business Regulatory Enforcement Fairness Act
V. Agency Regulatory Goal

12 CFR PART 748

Guidelines for Safeguarding Member Information

Read the Guidance at

https://www.ffiec.gov/exam/infobase/documents/02-ncu-12_cfr_748_app_a_safeguard_info-010100.pdf

Tandem™

EXAM PLATFORM

Instructions

Note: Gray cells are populated when the completed box is checked on the associated questionnaire.

The National Credit Union Administration is committed to providing access to all individuals — with or without disabilities, if you have difficulty accessing information in this document, please contact us at (703) 518-6372.

data and/or use this dropd

Required - All FCU and FISCU Exams

Required - SCUEP Exams (FCU & FISCU) — Use?

- Financial Triggers
- IC - Cash
- Red Flag Questionnaire
- Data-Network Controls

Required-RFE & ONES Exms (FCU&FISCU) — Use?

- CECL Preparedness

Required - RFE FCU Exams < $250 Million — Use?

- IT - 748A Information Security

Required - Exams - RFE FISCU < $250 Million &
RFE FCU & FISCU > $250 Million &
ONES FCU & FISCU &
previously received an ACET Review

- IT-Expanded 748 Compliance

Required - RFE FCU & FISCU Exams > $250 Million and have not previously received an ACET Review

- ACET

Required - SCUEP FCU Exams & Baseline - Non SCUEP FCU Exams — Use?

Additional — Use?

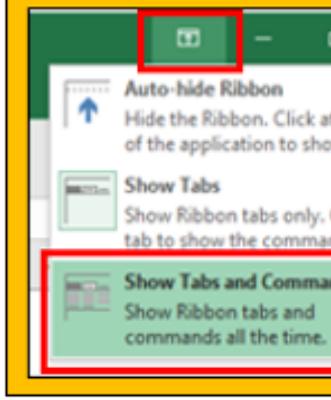
- IC - Wire Transfers
- ID Theft Red Flag Procedures
- Inv - Accounting Con
- Inv - Cash Forward
- Inv - CDs
- Inv - Controls
- Inv - Counter-Party Risk
- Inv - Derivatives
- Inv - Fed Funds
- Inv - IRPS 98-2
- Inv - Mutual Funds
- Inv - Repurchase
- Inv - Reverse Repo
- Inv - Safekeeping, B-D, Inv Adv
- Inv - SBA
- Inv - Securities Lending
- IT - 748A Items Needed
- IT - Website & E-banking
- Liquidity
- Ln - Agricultural - IC
- Ln - ARM - IC
- Ln - Business Loans - IC
- Ln - Collections - IC
- Ln - Construction - IC
- Ln - Credit Cards - IC

Additional — Use?

- Ln - Reg B - ECOA
- Ln - Reg C - HMDA
- Ln - Reg M - Leasing
- Ln - Reg X - RESPA
- Ln - Reg Z - TILA
- Ln - Reg Z - TILA - RESPA
- Ln - SBA
- Ln - SCRA
- Ln - Sub-Prime Lending - IC
- Non-Maturity Shares
- NWRP
- OFAC
- Physical Security
- Privacy
- Remote Dep Capture Procedures
- SAFE Act
- Sh - Controls
- Sh - IC
- Sh - Reg CC - Funds Avail
- Sh - Reg D - Reserve
- Sh - Reg E - EFT
- Sh - Share Drafts - IC
- Sh -TISA - Truth in Savings
- Third Party Relationships
- UIGEA Procedures

If all you see are the Tab
is set to Auto-hide like t

To return Excel back to
option button (little arro
and then click on Show



IT - 748A Items Needed

Comment to the Credit Union: This is a list of items needed for the IT review. Applicable items requested for this review are indicated with a "Yes". All items should be available at the start of the examination. Please number the items to correspond with the numbering system below, provide electronic versions of documents or reports, and include the lead contact person and phone number in the comment box. If an item is unavailable, please state why in the comment box.

	Description	Yes/No	Comments
1	Provide evidence of board involvement with the Information Security Program (ISP), for example: (1) approval of ISP; (2) Management Reports submitted to the board in the past year; and (3) technology committee minutes. (R&R 748 Appendix A III A)		
2	Provide copies of the last 2 reports presented to the Board of Directors on the overall status of your information security program. (R&R 748 Appendix A III F)		
3	Provide a current copy of your Risk Assessment and changes to this assessment within the last year. (R&R 748 Appendix A III B)		
4	Provide copies of IT audits and assessments conducted since the last examination as evidence of testing of key controls, systems, and operating procedures. (R&R 748 Appendix A III C)		
5	Provide a copy of your Information Security Program (R&R 748 Appendix A III C 1) and all applicable/related procedures not specifically requested below.		
5a	Provide, as applicable, policies, procedures, or operating standards/guidelines that indicate how access controls are designed to be an effective control mechanism. (R&R 748 Appendix A III C 1. a)		
5b	Provide, as applicable, policies, procedures, or		

Inv - SBA | Inv - Securities Lending | **IT - 748A Items Needed** | IT - Website & E-banking

IT - 748A Information Security

	INTRODUCTION AND PURPOSE		
	REGULATORY REFERENCES		
	Part 748 Appendix A - Information Security.	Yes/No/NA	Comment
1	Does the credit union have documented policies and procedures to address the implementation and ongoing management of the information security program?		
1a	Is the board of directors, or an appropriate board committee, involved in developing and implementing the Member Information Security Program ? (III. A)		
2	Does management report to the board of directors, at least annually, on the overall status of the information security program and compliance with Part 748, Appendix A and B guidelines? (III. F)		
3	Does the credit union have a documented risk assessment process that is updated annually? (III. B)		
4	Are key controls, systems, and operating procedures for the information security program regularly tested? (III. C. 3)		
5	Does the information security program address each of the following: (III. C. 1)		
5a	Electronic access controls on member information systems. (III. C. 1.a)		
5b	Physical access controls to facilities and equipment where data files and archives of member information are maintained. (III. C. 1.b)		
5c	Encryption of electronic member information either in transit or storage where unauthorized individuals may gain access. (III. C. 1.c)		
5d	Change control and update procedures designed to ensure system and/or software modifications are consistent with the credit union's information security program. (III. C. 1.d)		
5e	Dual control procedures, segregation of duties, and		

IC - Cash | Red Flag Questionnaire | Data-Network Controls | CECL Preparedness | Targe

rises, an institution's maturity levels should increase. An institution's inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change. Thus, management should consider reevaluating its inherent risk profile and cybersecurity maturity periodically and when planned changes can affect its inherent risk profile (e.g., launching new products or services, new connections).

Table 3: Risk/Maturity Relationship

Cybersecurity Maturity Level for Each Domain	Inherent Risk Levels: Least	Minimal	Moderate	Significant	Most
Innovative				■	■
Advanced			■	■	■
Intermediate		■	■	■	
Evolving	■	■	■		
Baseline	■	■			

If management determines that the institution's maturity levels are not appropriate in relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels. This process includes

- determining target maturity levels.
- conducting a gap analysis.
- prioritizing and planning actions.
- implementing changes.
- reevaluating over time.
- communicating the results.

Management can set target maturity levels for each domain or across domains based on the institution's business objectives and risk appetite. Management can conduct a gap analysis between the current and target maturity levels and initiate improvements based on the gaps. Each declarative statement can represent a range of strategies and processes that have enterprise-wide impact. For example, declarative statements not yet attained provide insights for policies, processes, procedures, and controls that may improve risk management in relation to a specific risk or the institution's overall cybersecurity preparedness.

Using the maturity levels in each domain, management can identify potential actions that would increase the institution's overall cybersecurity preparedness. Management can review declarative statements at maturity levels beyond what the institution has achieved to determine the actions needed to reach the next level and implement changes to address gaps. Management's periodic

FFIEC

Cybersecurity Assessment Tool

A Self Assessment

Download a Copy at
https://www.ffiec.gov/cyberassessmenttool.htm

Tandem

AIRES EXAM SPREADSHEET

EXAM TOPIC A

EXAM TOPIC B

EXAM TOPIC C

EXAM TOPIC D

IT - 748A InfoSec

DRL

EXAM TOPIC F

CAT

2015-2017

2001 – 2017

Tandem

NCUA SUPERVISORY PRIORITY LETTERS

2016

"In June 2015, NCUA released a Cybersecurity Assessment Tool [CAT] jointly with the other member agencies of the [FFIEC]. The tool provides a structured methodology for credit unions to manage information security [...] Credit unions can use this tool to enhance their cybersecurity preparedness. NCUA encourages all credit unions to use the FFIEC tool to manage cybersecurity risks. NCUA also plans to begin incorporating the [CAT] into our examination process in the second half of 2016."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/supervisory-priorities-2016

Tandem

NCUA SUPERVISORY PRIORITY LETTERS

2017

"We encourage credit unions to use [CAT] to bolster their security and risk management processes. This tool was issued jointly with the other member agencies of the [FFIEC]. NCUA plans to increase our emphasis on cybersecurity by enhancing the examination focus with a structured assessment process. We anticipate completing this process by late 2017, and will keep credit union system stakeholders informed as changes occur."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/supervisory-priorities-2017

Tandem

NCUA SUPERVISORY PRIORITY LETTERS

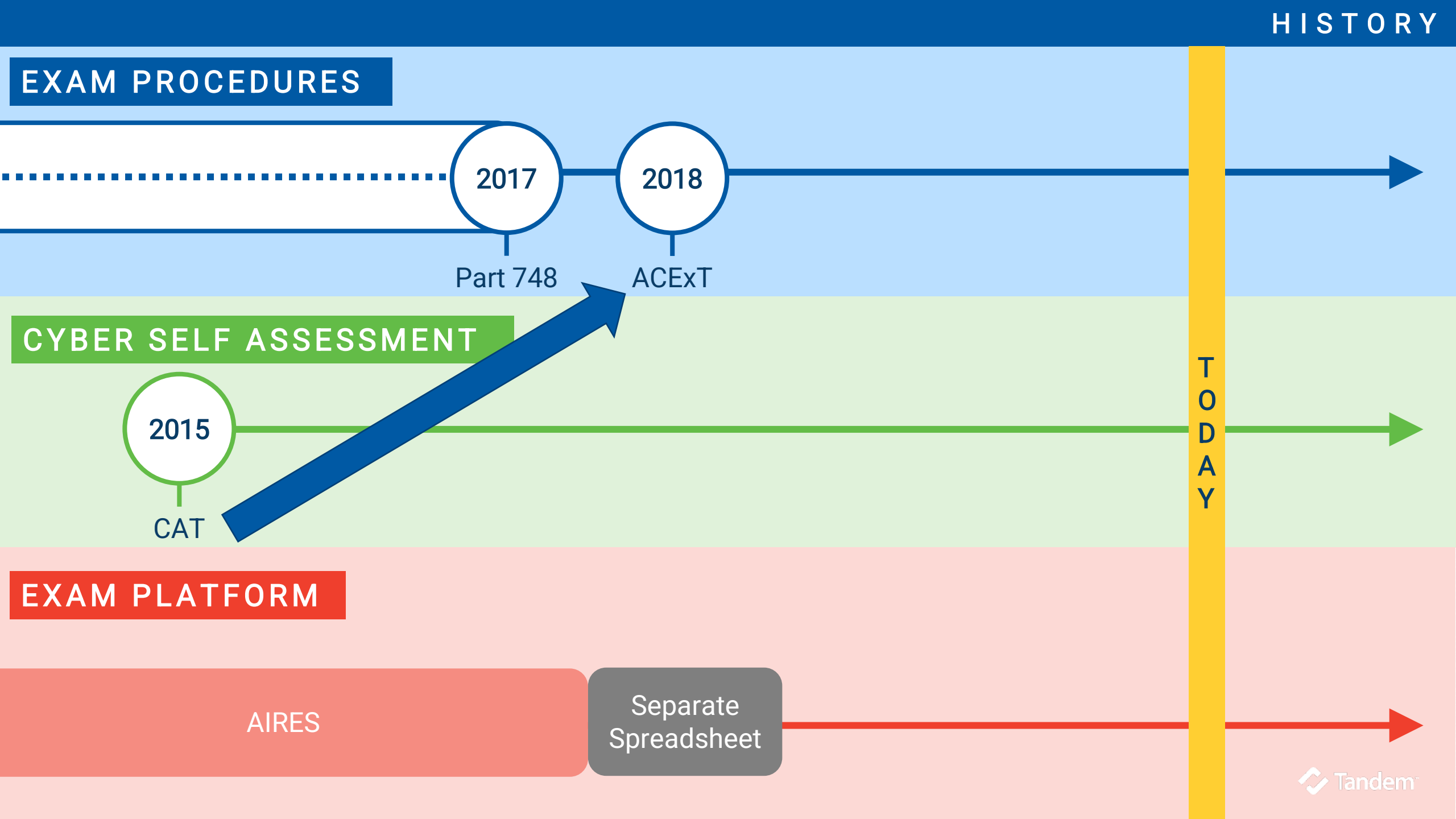
2018

"In 2018, the NCUA will begin implementing the Automated Cybersecurity Examination Tool (ACET) to improve and standardize supervision related to cybersecurity. The ACET provides the NCUA with a repeatable, measurable and transparent process for assessing the level of cyber preparedness across federally insured institutions. [] It also aligns with the [CAT] developed by the FFIEC for voluntary use by banks and [CUs]. Therefore, we encourage [CUs] to continue to self-assess their cybersecurity and risk management practices using the [CAT] if they do not have an alternative method of assessment.

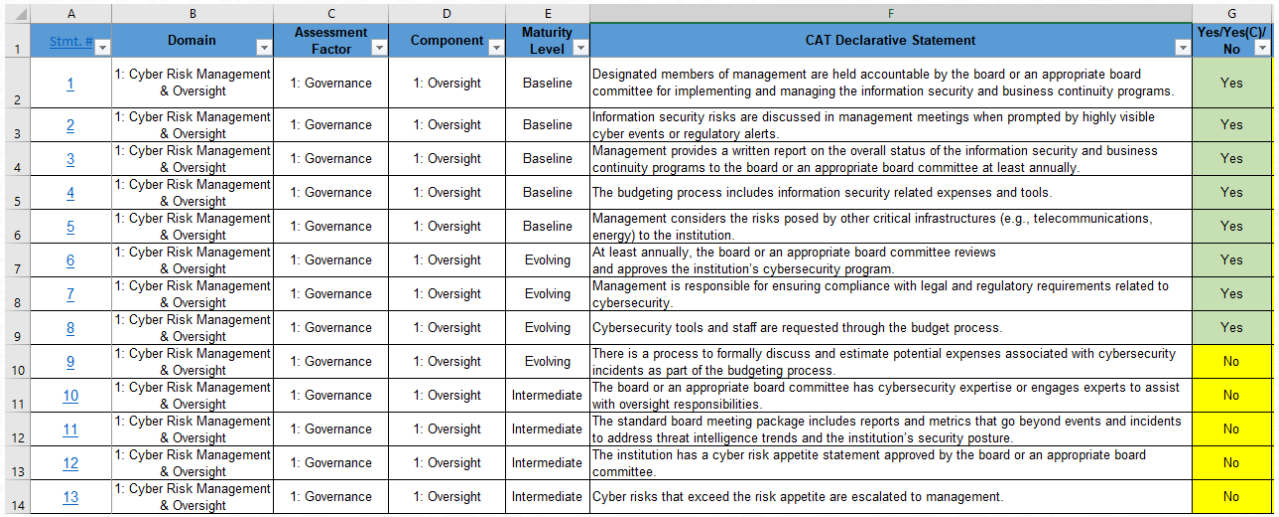
The NCUA will begin using the ACET in examinations of [CUs] with over $1 billion in assets. This will allow the NCUA to create a baseline for the cybersecurity maturity level of the largest and most complex institutions, while we continue to test and refine the ACET through 2018 to ensure it scales properly for smaller, less complex institutions."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/supervisory-priorities-2018

Tandem


HISTORY
EXAM PROCEDURES
2017
2018
Part 748
ACExT
CYBER SELF ASSESSMENT
2015
CAT
TODAY
EXAM PLATFORM
AIRES
Separate Spreadsheet
Tandem

NCUA



Stmt. #	Domain	Assessment Factor	Component	Maturity Level	CAT Declarative Statement	Yes/Yes(C)/ No
1	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.	Yes
2	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.	Yes
3	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.	Yes
4	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	The budgeting process includes information security related expenses and tools.	Yes
5	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution.	Yes
6	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Evolving	At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.	Yes
7	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Evolving	Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.	Yes
8	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Evolving	Cybersecurity tools and staff are requested through the budget process.	Yes
9	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Evolving	There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.	No
10	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities.	No
11	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The standard board meeting package includes reports and metrics that go beyond events and incidents to address threat intelligence trends and the institution's security posture.	No
12	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.	No
13	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	Cyber risks that exceed the risk appetite are escalated to management.	No

Automated Cybersecurity Examination Tool (ACExT)

An examination tool combining CAT and a document request list

Download a Copy at
https://go.tandem.app/ncua-acet/

Tandem

AIRES EXAM SPREADSHEET

EXAM TOPIC A

EXAM TOPIC B

EXAM TOPIC C

EXAM TOPIC D

ACExT

DRL

CAT

EXAM TOPIC F

2018

Tandem™

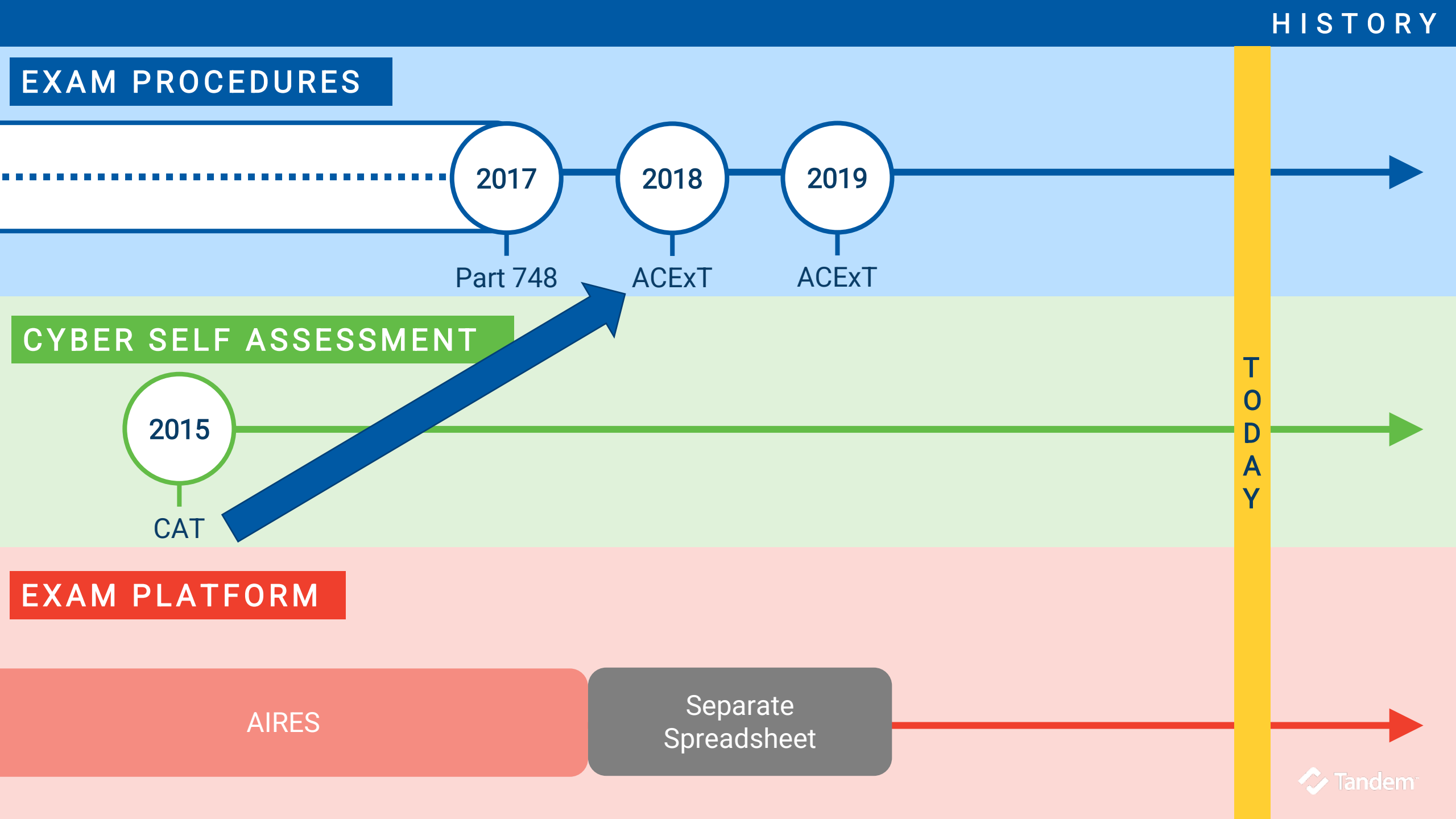
NCUA SUPERVISORY PRIORITY LETTERS

2019

"Examiners will continue conducting information security maturity assessments with the Automated Cybersecurity Examination Toolbox (ACET). Examiners will use the ACET to assess credit unions with over $250 million in assets that have not previously received an assessment."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/supervisory-priorities-2019

Tandem


HISTORY
EXAM PROCEDURES
2017
2018
2019
Part 748
ACExT
ACExT
CYBER SELF ASSESSMENT
2015
CAT
TODAY
EXAM PLATFORM
AIRES
Separate Spreadsheet
Tandem

2020

"In 2018, the NCUA began using the Automated Cybersecurity Examination Tool [ACET] to assess credit unions' cybersecurity maturity. The NCUA collaborated with the [DHS & INL] to create an updated client/server version of the ACET that is being fully deployed in 2020. Credit unions will be able to complete self-assessments through access to the new ACET on NCUA's website in early 2020. Starting in 2022, the agency will refresh the maturity assessments […] resulting in a refresh cycle of once every four years. In addition to the ACET, the NCUA will be piloting new procedures in 2020 to evaluate critical security controls during examinations between maturity assessments."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/2020-supervisory-priorities

NCUA SUPERVISORY PRIORITY LETTERS

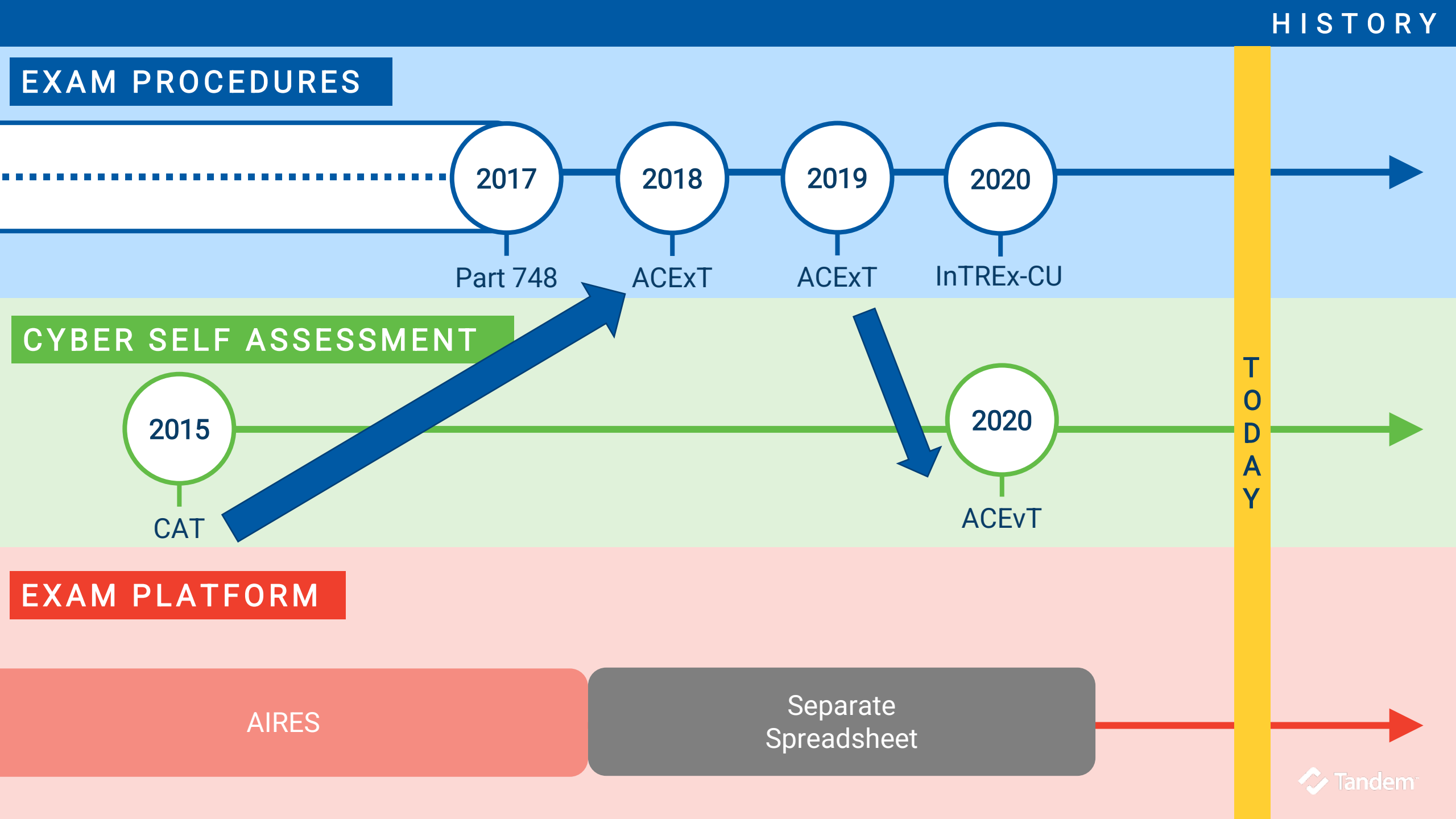
2020

UPDATED JULY

"The NCUA has transitioned its priority from performing Automated Cybersecurity Examination Tool (ACExT) cybersecurity maturity assessments, to evaluating critical security controls. The NCUA is also piloting an Information Technology Risk Examination solution for Credit Unions (InTREx-CU). InTREx-CU harmonizes the IT and Cybersecurity examination procedures shared by [other] regulators to ensure consistent approaches are applied to community financial institutions. The InTREx-CU will be deployed to identify gaps in security safeguards, allowing examiners and credit unions to identify and remediate potential high-risk areas through the identification of critical information security program deficiencies as represented by an array of critical security controls and practices."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/update-ncuas-2020-supervisory-priorities

Tandem


HISTORY
EXAM PROCEDURES
2017
2018
2019
2020
Part 748
ACExT
ACExT
InTREx-CU
CYBER SELF ASSESSMENT
2015
2020
CAT
ACEvT
TODAY
EXAM PLATFORM
AIRES
Separate
Spreadsheet
Tandem

EXAM PROCEDURES

#	Document Request
IT 01	Provide the IT Audit risk assessment, and any other related supporting documentation.
IT 02	Provide the audit schedule and documentation demonstrating the board or committee approve the audit schedule.
IT 03	Provide all IT Audit reports and/or results from independent IT control testing conducted in the last 12 months
IT 04	Provide reports and meeting minutes presented to the board or committee demonstrating the types of reports and information presented by Audit. Additionally, an org chart depicting the full reporting structure of all audit staff.
IT 05	Provide documentation/reports supporting the process used by Audit/Supervisory Committee to manage and monitor IT Audit findings.
IT 06	Provide the formal Information Security Program/Policy and all other supporting Policies/Procedures/Practices; such as; policies/procedures addressing acceptable use, business continuity, access controls, electronic funds transfer, remote access, bring your own device (BYOD),
IT 07	Provide the most current Annual Report to the Board regarding regarding the overall status of the Information Security Program
IT 08	Provide Organizational Chart depicting all IT Security and IT Operations staff and positions.
IT 09	Provide documentation demonstrating how management resolves and monitors corrective actions noted within IT examination reports, audits, service provider/vendor reviews, and internal reviews (e.g., disaster recovery, incident response, penetration testing, cybersecurity tests).
IT 10	Provide the results and documentation supporting the information security risk assessment.
IT 11	Provide results from all security awareness training activities provided to staff and customers/members in the last 12 months.

InTREx-CU Required | DRL - Required | InTREx-CU Optional | InTREx-CU Expanded

InTREx-CU

Information Technology Risk Examination for Credit Unions

Read more at

https://tandem.app/blog/how-intrex-cu-will-affect-your-2022-ncua-exam

Tandem

AIRES EXAM SPREADSHEET

EXAM TOPIC A

EXAM TOPIC B

EXAM TOPIC C

EXAM TOPIC D

InTREx CU

DRL

PILOT

XAM TOPIC F

ACEvT

CAT

2020

Tandem

AIRES EXAM SPREADSHEET

EXAM TOPIC A

EXAM TOPIC B

EXAM TOPIC C

EXAM TOPIC D

InTREx-CU

DRL

PILOT

OR

IT - 748A

DRL

EXAM TOPIC F

ACEvT

CAT

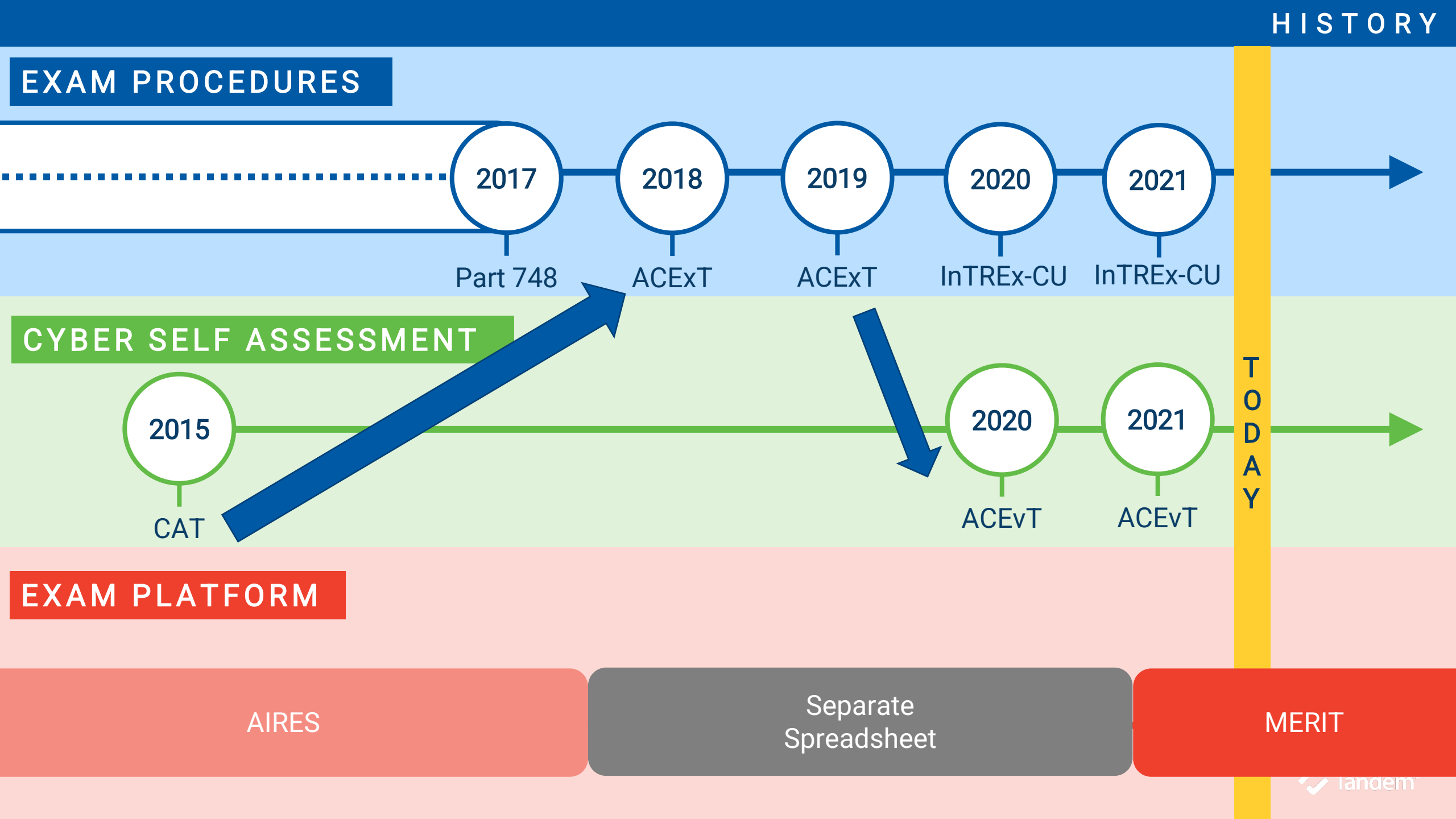
2020

Tandem

2021

"As cited in the NCUA's updated supervisory priorities for 2020, the agency has reprioritized away from performing facilitated Automated Cybersecurity Evaluation Toolbox (ACET) cybersecurity maturity assessments, to piloting the Information Technology Risk Examination for Credit Unions (InTREx-CU). InTREx-CU harmonizes the IT and cybersecurity examination procedures shared by [other] regulators. This establishes a consistent approach across all community-based financial institutions. The InTREx-CU will continue to be deployed in 2021, allowing examiners and credit unions to identify and remediate potential high-risk areas by identifying critical information security program deficiencies. ACEvT will become a self-assessment resource for credit unions, supported by the NCUA."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/ncuas-2021-supervisory-priorities


HISTORY
EXAM PROCEDURES
2017
2018
2019
2020
2021
Part 748
ACExT
ACExT
InTREx-CU
InTREx-CU
CYBER SELF ASSESSMENT
2015
2020
2021
CAT
ACEvT
ACEvT
TODAY
EXAM PLATFORM
AIRES
Separate Spreadsheet
MERIT

NCUA LETTER 21-CU-08

21-CU-08

This letter provides important updates regarding the NCUA's recent technology modernization efforts and outlines the implementation of key software tools.

In August, the NCUA will begin transitioning to several new modernized applications, which are listed below. […] Modern Examination & Risk Identification Tool (MERIT).

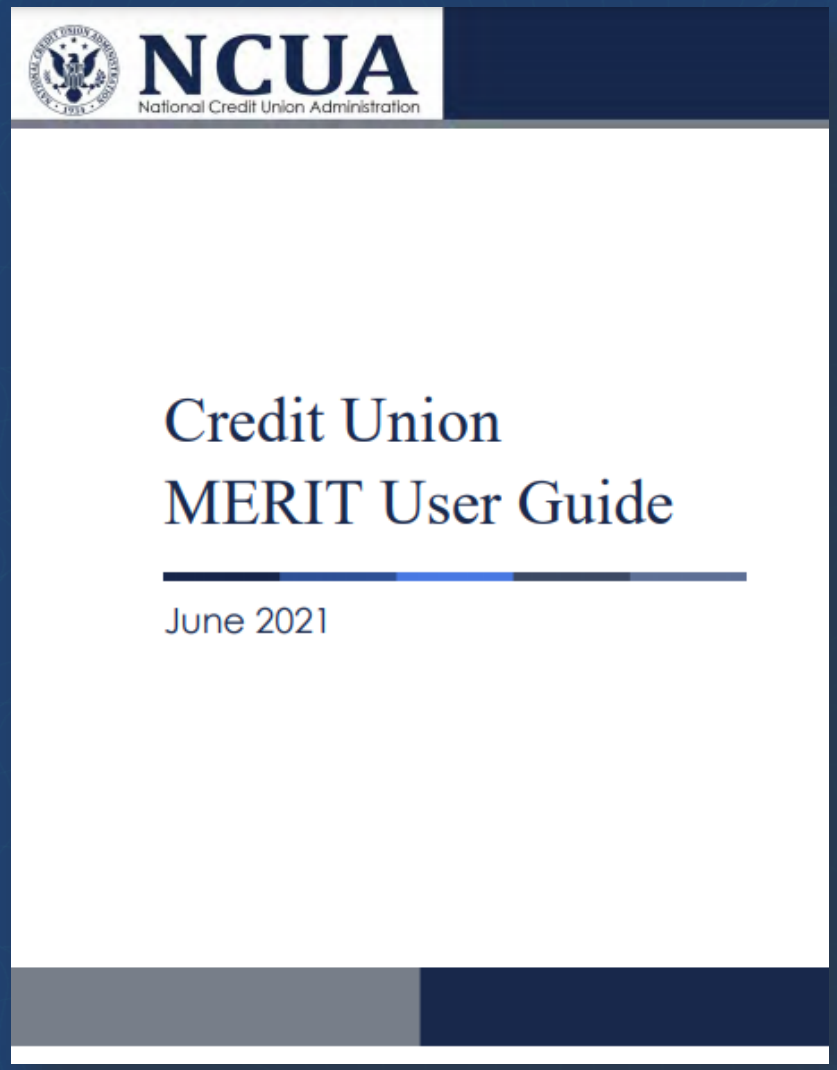
https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/implementation-modernized-systems

Tandem™

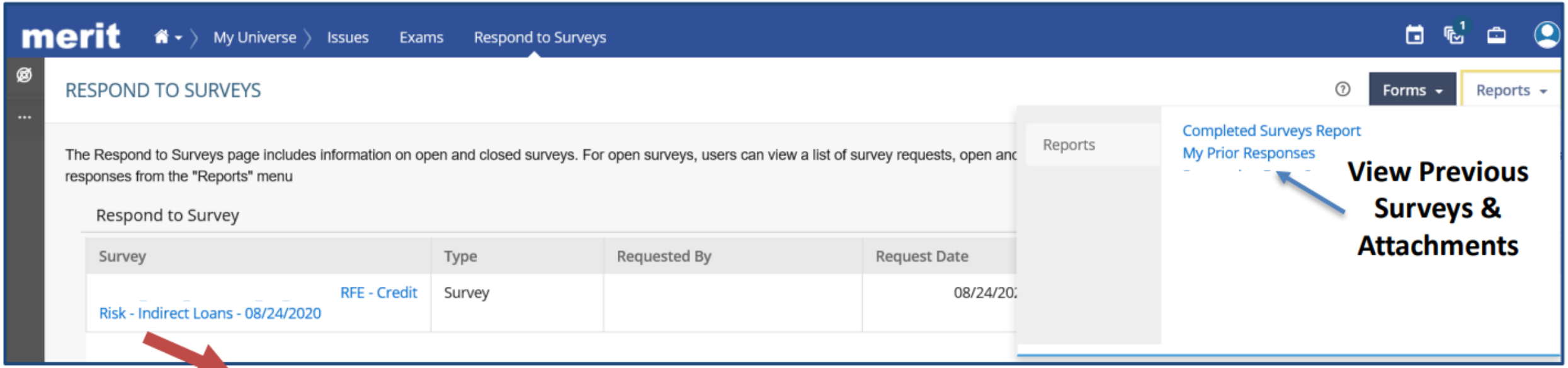
merit
MODERN EXAMINATION & RISK IDENTIFICATION TOOL

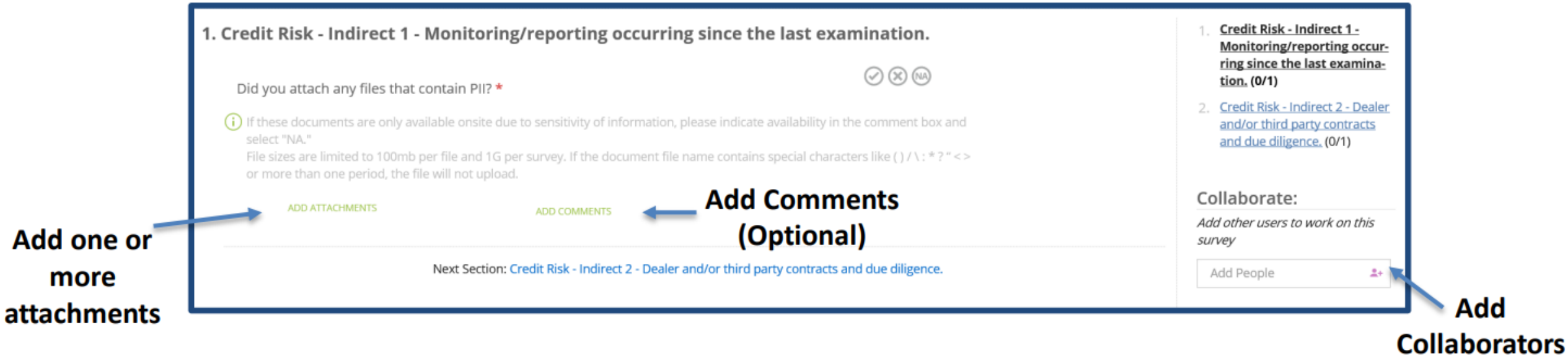
LEARN MORE

https://www.ncua.gov/regulation-supervision/examination-modernization-initiatives/enterprise-solution-modernization-program/modern-examination-risk-identification-tool



Tandem


merit
My Universe
Issues
Exams
Respond to Surveys
RESPOND TO SURVEYS
Forms
Reports
The Respond to Surveys page includes information on open and closed surveys. For open surveys, users can view a list of survey requests, open and
responses from the "Reports" menu
Respond to Survey
Survey
Type
Requested By
Request Date
RFE - Credit Risk - Indirect Loans - 08/24/2020
Survey
08/24/20
Reports
Completed Surveys Report
My Prior Responses
View Previous Surveys & Attachments


1. Credit Risk - Indirect 1 - Monitoring/reporting occurring since the last examination.
Did you attach any files that contain PII? *
If these documents are only available onsite due to sensitivity of information, please indicate availability in the comment box and select "NA."
File sizes are limited to 100mb per file and 1G per survey. If the document file name contains special characters like ( ) / \ : * ? " < > or more than one period, the file will not upload.
ADD ATTACHMENTS
ADD COMMENTS
Add Comments (Optional)
Add one or more attachments
Next Section: Credit Risk - Indirect 2 - Dealer and/or third party contracts and due diligence.
1. Credit Risk - Indirect 1 - Monitoring/reporting occurring since the last examination. (0/1)
2. Credit Risk - Indirect 2 - Dealer and/or third party contracts and due diligence. (0/1)
Collaborate:
Add other users to work on this survey
Add People
Add Collaborators

Tandem

MERIT EXAM WEB APPLICATION

EXAM TOPIC A

EXAM TOPIC B

EXAM TOPIC C

EXAM TOPIC D

InTREx-CU

DRL

PILOT

OR

IT - 748A

DRL

EXAM TOPIC F

ACEvT

CAT

2021

Tandem

National Credit Union Administration

Search NCUA.gov Go

Locate a credit union | Research a credit union

About > Regulation & Supervision > Analysis > Support Services > Consumers > News > COVID-19 >

Home > Regulation and Supervision > Regulatory and Compliance Resources > Cybersecurity Resources

Cybersecurity Resources

- NCUA's Information Security Examination and Cybersecurity Assessment Program
- ACET and Other Assessment Tools
- Supply Chain Risk Management (SCRM)
- Catastrophic and Incident Reporting
- NCUA's Regulations and Guidance
- References & Resources

ACET and Other Assessment Tools

ACET
AUTOMATED CYBERSECURITY EVALUATION TOOLBOX

The NCUA's ACET (Automated Cybersecurity Evaluation Toolbox) application provides credit unions the capability to conduct a maturity assessment aligned with the Federal Financial Information Council's (FFIEC) Cybersecurity Assessment Tool. Using the assessment within the toolbox allows institutions of all sizes to easily determine and measure their own cybersecurity preparedness over time.

The ACET self-assessment is completely voluntary and does not introduce any new requirements or expectations on credit unions. It is simply a tool that allows credit unions to identify and determine their levels of cybersecurity preparedness.

Using the Toolbox to conduct assessments on a regular basis may help institutions to:

https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources/acet-and-other-assessment-tools

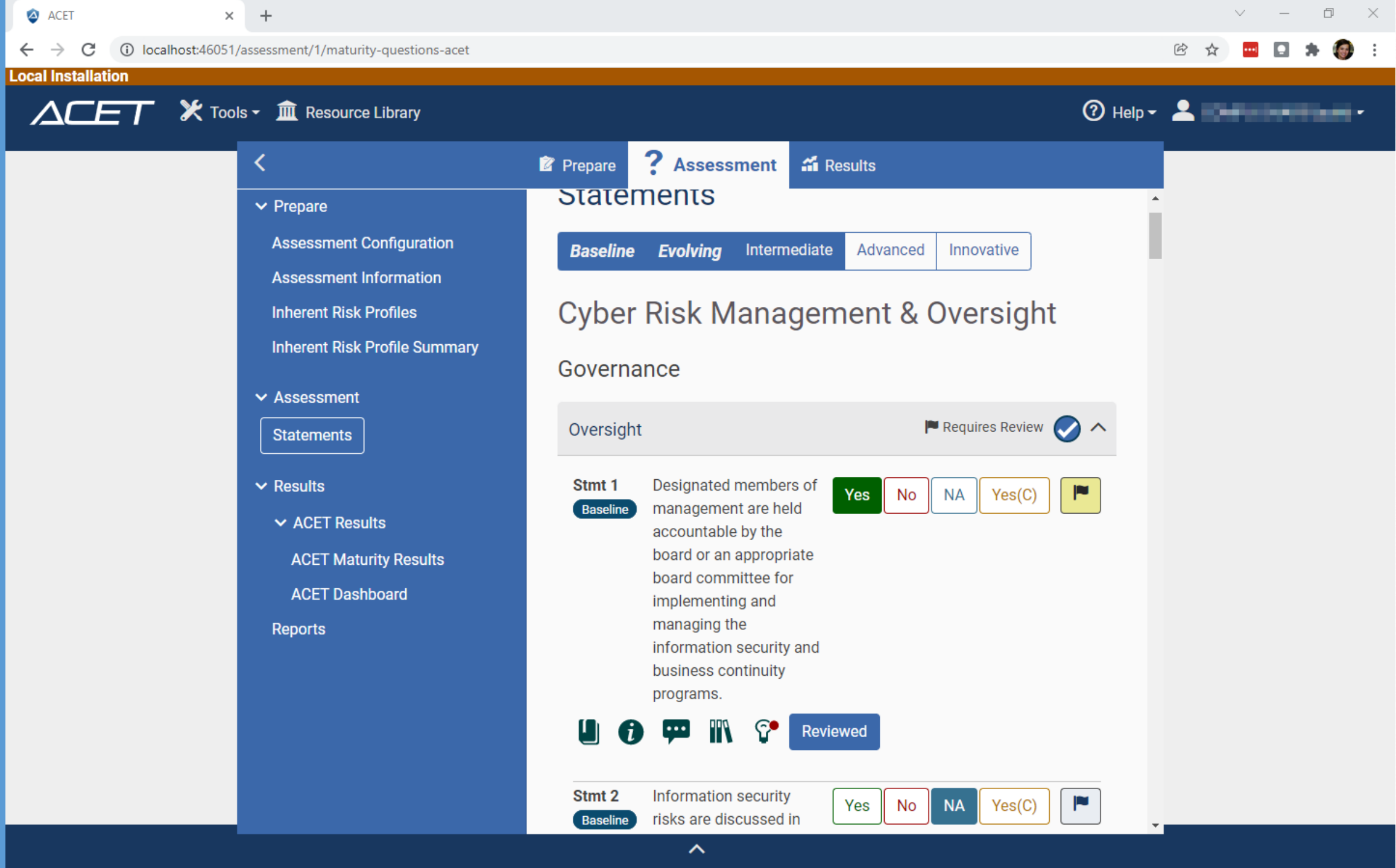
Tandem

- Is there a cost to downloading, installing, and using the ACET Toolbox application?
- Are credit unions required to complete the ACET maturity assessment?
- Does the ACET maturity assessment replace the risk assessment process outlined in the Gramm-Leach-Bliley Act (GLBA) Guidelines?
- Is the ACET maturity assessment the IT examination?
- Are examiners able to assist credit unions in completing the ACET maturity assessment?
- What value does the ACET maturity assessment module provide to credit unions?
- How do I use the ACET maturity assessment within the Toolbox?
- Where is information collected from the ACET maturity assessment stored?

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/automated-cybersecurity-evaluation-toolbox/frequently-asked-questions

Tandem™

Sample ACEvT Local App



Tandem

NCUA COMMENTARY

STATEMENT FROM NCUA REPRESENTATIVE DURING ACET WEBINAR ON 10/28/21

InTREx-CU will not be a permanent examination solution. Instead, results from InTREx-CU exams will be used to improve the existing examination program. The updated Part 748 exam program will be used starting in September 2022.

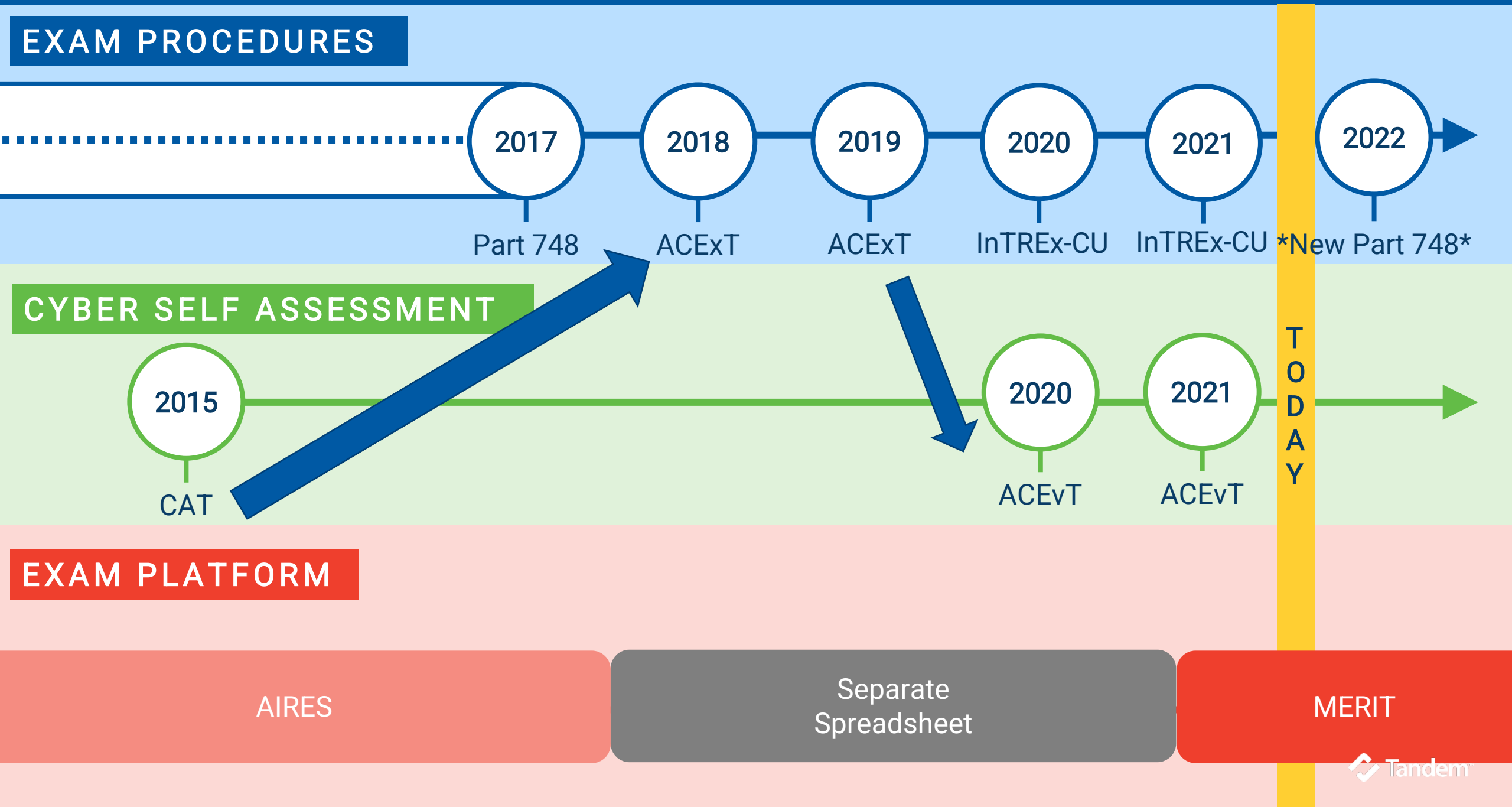
Tandem

2022

"The NCUA continues to develop updated information security examination procedures that are tailored to institutions of varying size and complexity. These procedures will continue to be piloted in 2022, with the goal of having them finalized in 2022.

In October 2021, the NCUA released the Automated Cybersecurity Evaluation Toolbox (ACET) application, which provides credit unions the capability to conduct a maturity assessment aligned with the [FFIEC] Cybersecurity Assessment Tool. Using the assessment within the ACET allows institutions of all sizes to determine and measure their cybersecurity preparedness. The ACET is entirely voluntary and does not introduce any new requirements or expectations on credit unions."

https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/ncuas-2022-supervisory-priorities


EXAM PROCEDURES
2017
2018
2019
2020
2021
2022
Part 748
ACExT
ACExT
InTREx-CU
InTREx-CU
New Part 748
CYBER SELF ASSESSMENT
2015
2020
2021
CAT
ACEvT
ACEvT
TODAY
EXAM PLATFORM
AIRES
Separate Spreadsheet
MERIT

Tandem

MERIT EXAM WEB APPLICATION

EXAM TOPIC A

EXAM TOPIC B

EXAM TOPIC C

EXAM TOPIC D

NEW PART 748

DRL

EXAM TOPIC F

ACEvT

CAT

By end of 2022

Tandem

What to Expect in Your 2022 Exam

Tandem

EXAM PLATFORM

EXPECT to have your exam conducted using the **MERIT web application**.

Do not expect to have your exam conducted using the **AIRES spreadsheet**.

EXAM PROCEDURES

EXPECT to have your exam conducted using the traditional **Part 748** exam procedures until, probably, end of 2022 where there will be a **NEW Part 748** version.

Do not expect to have your exam conducted using **ACExT or InTREx-CU.** *Exception: if you are scheduled to be examined by a RISO, they may use InTREx-CU.*

CYBER SELF ASSESSMENT

EXPECT to have the NCUA *recommend* you complete a **cybersecurity self-assessment** (with ACEvT or similar tool) to measure your cybersecurity maturity.

Do not expect to have the NCUA ask you for the **results** of any CAT assessment as part of your exam.

Tandem™

How Tandem Addresses These Expectations

Tandem

F A Q

Will Tandem offer a Document Request list feature for the new IT 748 exam?

Maybe, if use of the MERIT application proves difficult and us building a tool will help our Credit Unions.

ACEvT Application Options

ACExT
Spreadsheet

Tandem
Cybersecurity
Product

ACEvT
Desktop
Application

Tandem

Feature Comparison	NCUA's ACExT Spreadsheet	NCUA's ACEvT Local App	Tandem's Cybersecurity Web App
Price	Free	Free	Free
Data management	Locally stored	Locally installed	SAAS
Data Backup	not provided	not provided	Provided
Includes All FFIEC CAT Questions	✓	✓	✓
Mirrors FFIEC CAT Answer Options	✓		✓
Download results in the ACExT Format	✓		✓
Guidance and NCUA Commentary	✓	✓	✓
A downloadable Report to the Board		✓	✓
Gap Reporting		✓	✓
Optional Peer Analysis			✓
Reports Branded for your Organization			✓
Built for Optimum Screen Usage			✓
Keyboard shortcut to answer questions			✓
Easy-to-Read Reports for Board of Directors			✓

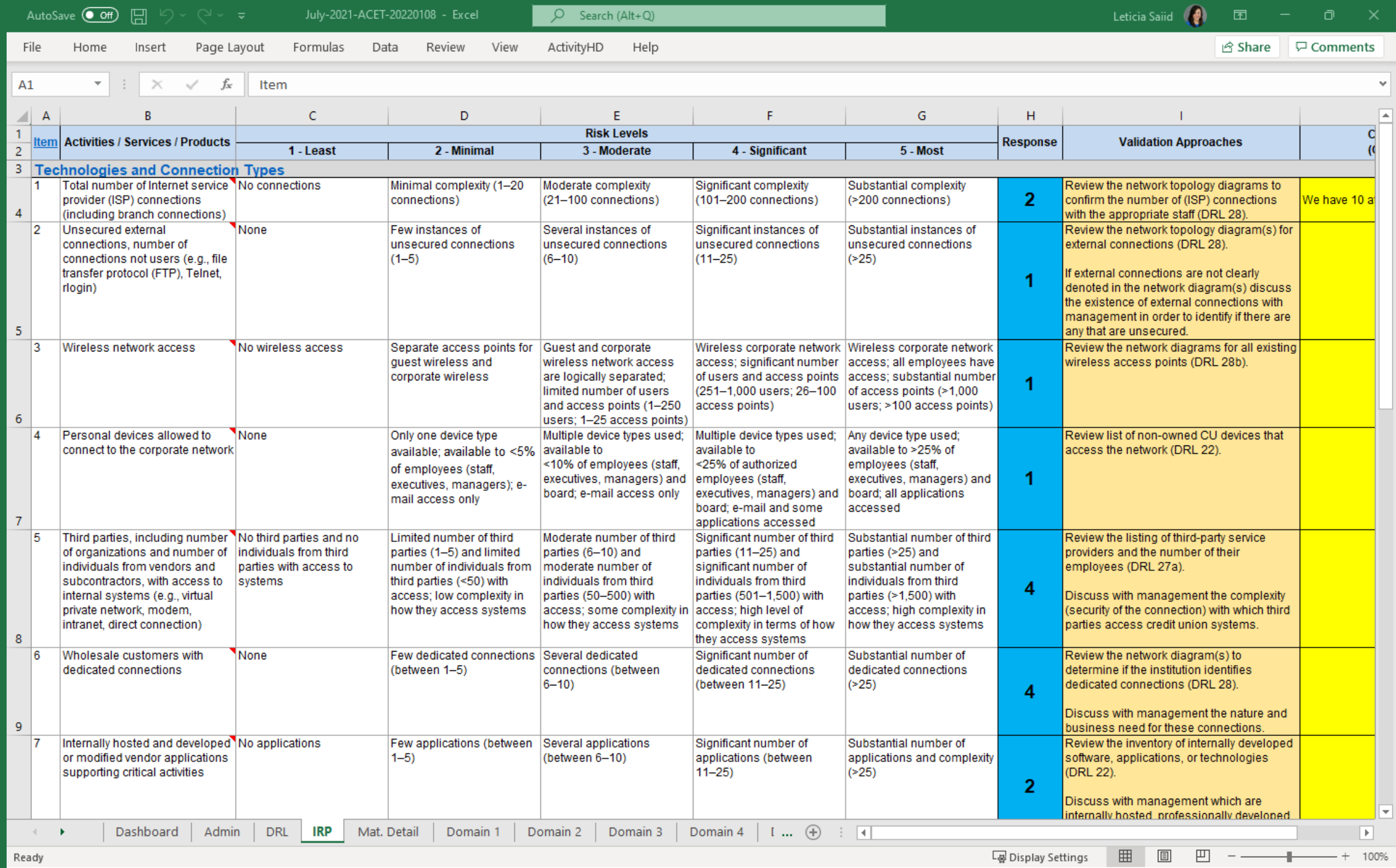
Tandem™

Tandem Cybersecurity Pro Features

- Custom User Responsibility and Notifications
- Filter Peer Data by Asset Size
- Download Peer Data
- File attachments
- Flag questions for follow up at a later time
- Revision/Approval Log
- Trend Reporting
- Copy to New
- And more

Tandem

Sample ACExT Spreadsheet



AutoSave Off | July-2021-ACET-20220108 - Excel | Search (Alt+Q) | Leticia Saiid

File Home Insert Page Layout Formulas Data Review View ActivityHD Help | Share | Comments

A1 | Item

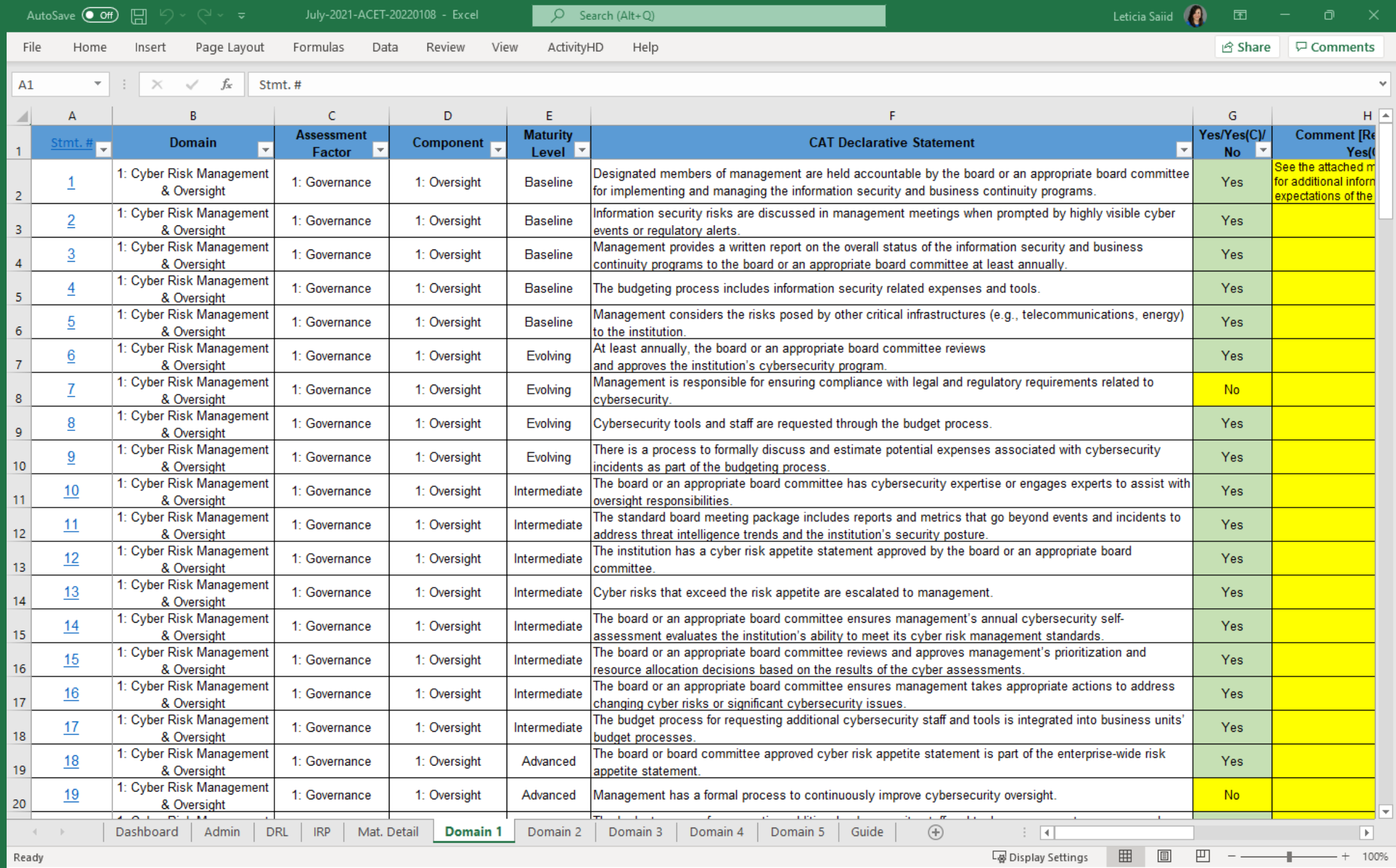
Item	Activities / Services / Products	Risk Levels 1 - Least	2 - Minimal	3 - Moderate	4 - Significant	5 - Most	Response	Validation Approaches	C ((
Technologies and Connection Types									
1	Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)	2	Review the network topology diagrams to confirm the number of (ISP) connections with the appropriate staff (DRL 28).	We have 10 a
2	Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)	1	Review the network topology diagram(s) for external connections (DRL 28). If external connections are not clearly denoted in the network diagram(s) discuss the existence of external connections with management in order to identify if there are any that are unsecured.	
3	Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)	1	Review the network diagrams for all existing wireless access points (DRL 28b).	
4	Personal devices allowed to connect to the corporate network	None	Only one device type available; available to <5% of employees (staff, executives, managers); e-mail access only	Multiple device types used; available to <10% of employees (staff, executives, managers) and board; e-mail access only	Multiple device types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed	Any device type used; available to >25% of employees (staff, executives, managers) and board; all applications accessed	1	Review list of non-owned CU devices that access the network (DRL 22).	
5	Third parties, including number of organizations and number of individuals from vendors and subcontractors, with access to internal systems (e.g., virtual private network, modem, intranet, direct connection)	No third parties and no individuals from third parties with access to systems	Limited number of third parties (1–5) and limited number of individuals from third parties (<50) with access; low complexity in how they access systems	Moderate number of third parties (6–10) and moderate number of individuals from third parties (50–500) with access; some complexity in how they access systems	Significant number of third parties (11–25) and significant number of individuals from third parties (501–1,500) with access; high level of complexity in terms of how they access systems	Substantial number of third parties (>25) and substantial number of individuals from third parties (>1,500) with access; high complexity in how they access systems	4	Review the listing of third-party service providers and the number of their employees (DRL 27a). Discuss with management the complexity (security of the connection) with which third parties access credit union systems.	
6	Wholesale customers with dedicated connections	None	Few dedicated connections (between 1–5)	Several dedicated connections (between 6–10)	Significant number of dedicated connections (between 11–25)	Substantial number of dedicated connections (>25)	4	Review the network diagram(s) to determine if the institution identifies dedicated connections (DRL 28). Discuss with management the nature and business need for these connections.	
7	Internally hosted and developed or modified vendor applications supporting critical activities	No applications	Few applications (between 1–5)	Several applications (between 6–10)	Significant number of applications (between 11–25)	Substantial number of applications and complexity (>25)	2	Review the inventory of internally developed software, applications, or technologies (DRL 22). Discuss with management which are internally hosted, professionally developed	

Dashboard | Admin | DRL | IRP | Mat. Detail | Domain 1 | Domain 2 | Domain 3 | Domain 4 | ...

Ready | Display Settings | 100%

Tandem

Sample ACExT Spreadsheet



AutoSave Off | July-2021-ACET-20220108 - Excel | Search (Alt+Q) | Leticia Saiid

File Home Insert Page Layout Formulas Data Review View ActivityHD Help | Share | Comments

A1 | Stmt. #

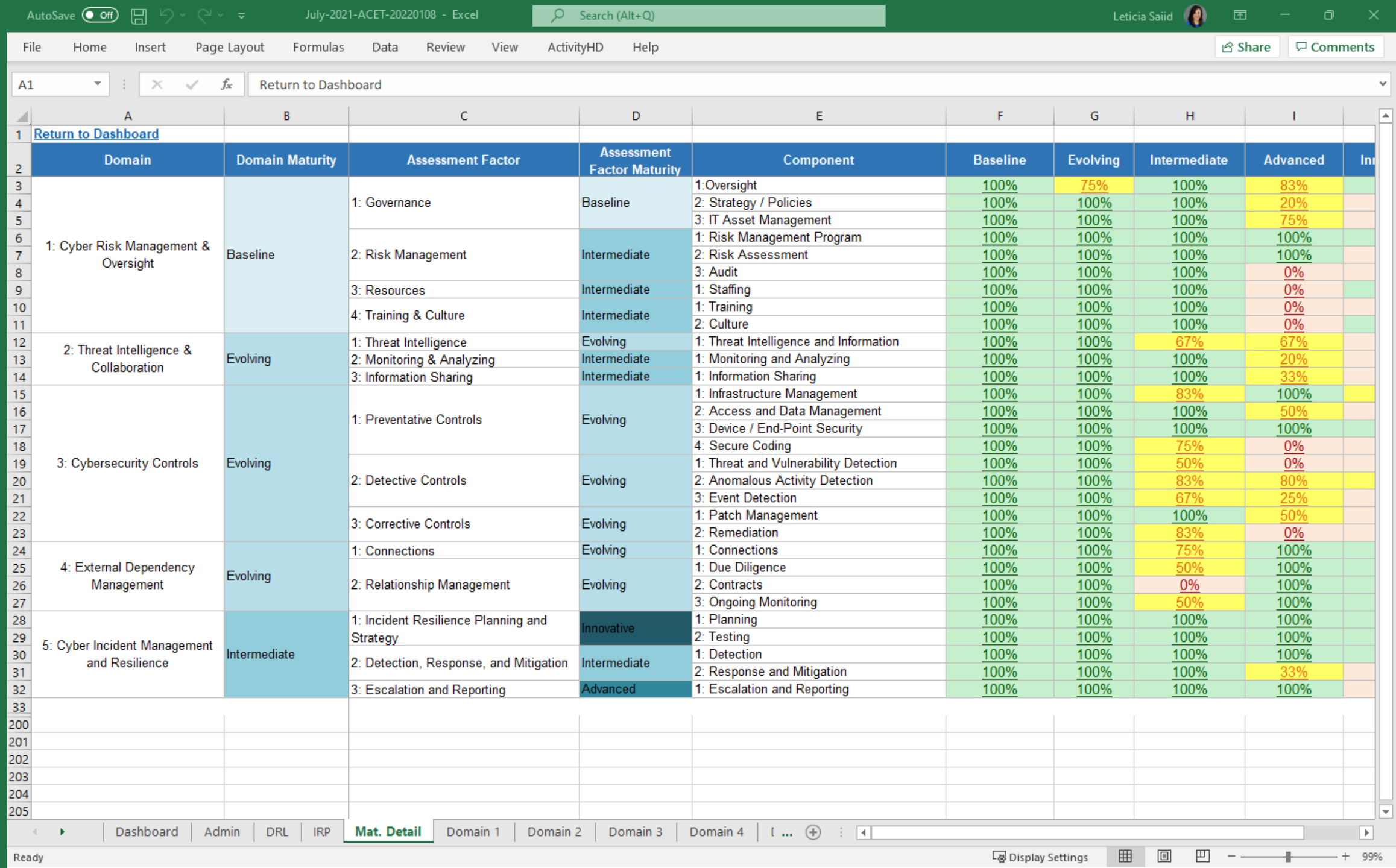
Stmt. #	Domain	Assessment Factor	Component	Maturity Level	CAT Declarative Statement	Yes/Yes(C)/ No	Comment [Re Yes(
1	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.	Yes	See the attached m for additional inform expectations of the
2	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.	Yes	
3	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.	Yes	
4	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	The budgeting process includes information security related expenses and tools.	Yes	
5	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution.	Yes	
6	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Evolving	At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.	Yes	
7	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Evolving	Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.	No	
8	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Evolving	Cybersecurity tools and staff are requested through the budget process.	Yes	
9	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Evolving	There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.	Yes	
10	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities.	Yes	
11	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The standard board meeting package includes reports and metrics that go beyond events and incidents to address threat intelligence trends and the institution's security posture.	Yes	
12	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.	Yes	
13	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	Cyber risks that exceed the risk appetite are escalated to management.	Yes	
14	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards.	Yes	
15	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The board or an appropriate board committee reviews and approves management's prioritization and resource allocation decisions based on the results of the cyber assessments.	Yes	
16	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The board or an appropriate board committee ensures management takes appropriate actions to address changing cyber risks or significant cybersecurity issues.	Yes	
17	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Intermediate	The budget process for requesting additional cybersecurity staff and tools is integrated into business units' budget processes.	Yes	
18	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Advanced	The board or board committee approved cyber risk appetite statement is part of the enterprise-wide risk appetite statement.	Yes	
19	1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Advanced	Management has a formal process to continuously improve cybersecurity oversight.	No	

Dashboard | Admin | DRL | IRP | Mat. Detail | Domain 1 | Domain 2 | Domain 3 | Domain 4 | Domain 5 | Guide

Ready | Display Settings | 100%

Tandem

Sample ACExT Spreadsheet



AutoSave Off | July-2021-ACET-20220108 - Excel | Search (Alt+Q) | Leticia Saiid

File Home Insert Page Layout Formulas Data Review View ActivityHD Help | Share | Comments

A1 | Return to Dashboard

Return to Dashboard

Domain	Domain Maturity	Assessment Factor	Assessment Factor Maturity	Component	Baseline	Evolving	Intermediate	Advanced	Inn
1: Cyber Risk Management & Oversight	Baseline	1: Governance	Baseline	1:Oversight	100%	75%	100%	83%	
				2: Strategy / Policies	100%	100%	100%	20%	
				3: IT Asset Management	100%	100%	100%	75%	
		2: Risk Management	Intermediate	1: Risk Management Program	100%	100%	100%	100%	
				2: Risk Assessment	100%	100%	100%	100%	
				3: Audit	100%	100%	100%	0%	
		3: Resources	Intermediate	1: Staffing	100%	100%	100%	0%	
		4: Training & Culture	Intermediate	1: Training	100%	100%	100%	0%	
				2: Culture	100%	100%	100%	0%	
2: Threat Intelligence & Collaboration	Evolving	1: Threat Intelligence	Evolving	1: Threat Intelligence and Information	100%	100%	67%	67%	
		2: Monitoring & Analyzing	Intermediate	1: Monitoring and Analyzing	100%	100%	100%	20%	
		3: Information Sharing	Intermediate	1: Information Sharing	100%	100%	100%	33%	
3: Cybersecurity Controls	Evolving	1: Preventative Controls	Evolving	1: Infrastructure Management	100%	100%	83%	100%	
				2: Access and Data Management	100%	100%	100%	50%	
				3: Device / End-Point Security	100%	100%	100%	100%	
				4: Secure Coding	100%	100%	75%	0%	
		2: Detective Controls	Evolving	1: Threat and Vulnerability Detection	100%	100%	50%	0%	
				2: Anomalous Activity Detection	100%	100%	83%	80%	
				3: Event Detection	100%	100%	67%	25%	
		3: Corrective Controls	Evolving	1: Patch Management	100%	100%	100%	50%	
				2: Remediation	100%	100%	83%	0%	
4: External Dependency Management	Evolving	1: Connections	Evolving	1: Connections	100%	100%	75%	100%	
		2: Relationship Management	Evolving	1: Due Diligence	100%	100%	50%	100%	
				2: Contracts	100%	100%	0%	100%	
				3: Ongoing Monitoring	100%	100%	50%	100%	
5: Cyber Incident Management and Resilience	Intermediate	1: Incident Resilience Planning and Strategy	Innovative	1: Planning	100%	100%	100%	100%	
				2: Testing	100%	100%	100%	100%	
		2: Detection, Response, and Mitigation	Intermediate	1: Detection	100%	100%	100%	100%	
				2: Response and Mitigation	100%	100%	100%	33%	
		3: Escalation and Reporting	Advanced	1: Escalation and Reporting	100%	100%	100%	100%	

Dashboard | Admin | DRL | IRP | Mat. Detail | Domain 1 | Domain 2 | Domain 3 | Domain 4 | ...

Ready | Display Settings | 99%

Tandem

Sample ACExT Spreadsheet

A1 | Automated Cybersecurity Assessment Tool (ACET) Version 1.0

Automated Cybersecurity Assessment Tool (ACET) Version 1.0

Exam Preparation

Administrative Tab (Admin)

Document Request List (DRL)

Credit Union Name:	Tandem Financial
Charter:	
Assets:	
Hours:	0.0

Inherent Risk Profile (IRP)

Category	Inherent Risk 1	2	3	4	5	Total Items	Risk Level
Technologies and Connection Types	7	3	1	3	0	14	2 - Minimal
Delivery Channels	0	0	0	1	2	3	5 - Most
Online/Mobile Products and Technology Services	2	2	5	2	3	14	3 - Moderate
Organizational Characteristics	2	2	1	2	0	7	4 - Significant
External Threats	1	0	0	0	0	1	1 - Least
Total	**12**	**7**	**7**	**8**	**5**	**39**	**Complete**

Note: You must assign risk levels for each category based on the risk ratings tabulated from the IRP worksheet.

Cybersecurity Maturity

Domain	Maturity Level
Domain 1: Cyber Risk Management & Oversight	Baseline
Domain 2: Threat Intelligence & Collaboration	Evolving
Domain 3: Cybersecurity Controls	Evolving
Domain 4: External Dependency Management	Evolving
Domain 5: Cyber Incident Management and Resilience	Intermediate

Click here to see detail

Note: The maturity levels are automatically calculated based on the responses in the Domain worksheets.

V1.0.032618

Tandem

Sample ACEvT Local App

ACET

localhost:[redacted]/home/landing-page

Local Installation

ACET Tools Resource Library Help [redacted]

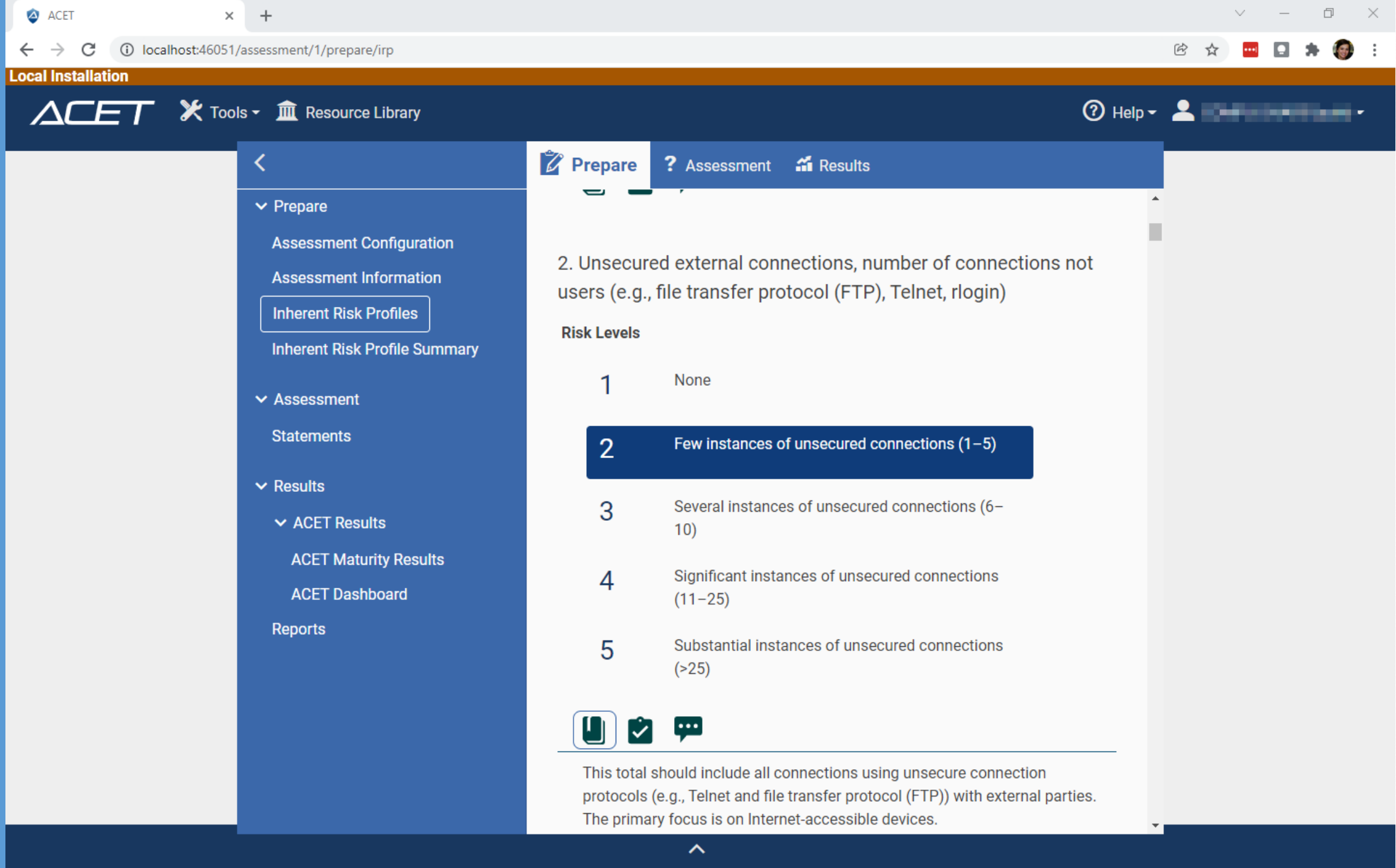
My Assessments

New Assessment | Import | Export All to Excel

Assessment Name	Last Modified	Primary Assessor	Status	
ACET 55555 CoNetrix DBA Tandem Financial etc. 102821	06-Jan-2022	[redacted]	Needs Review	Remove Export
ACET 00000 CoNetrix 120621	06-Dec-2021	[redacted]		Remove Export

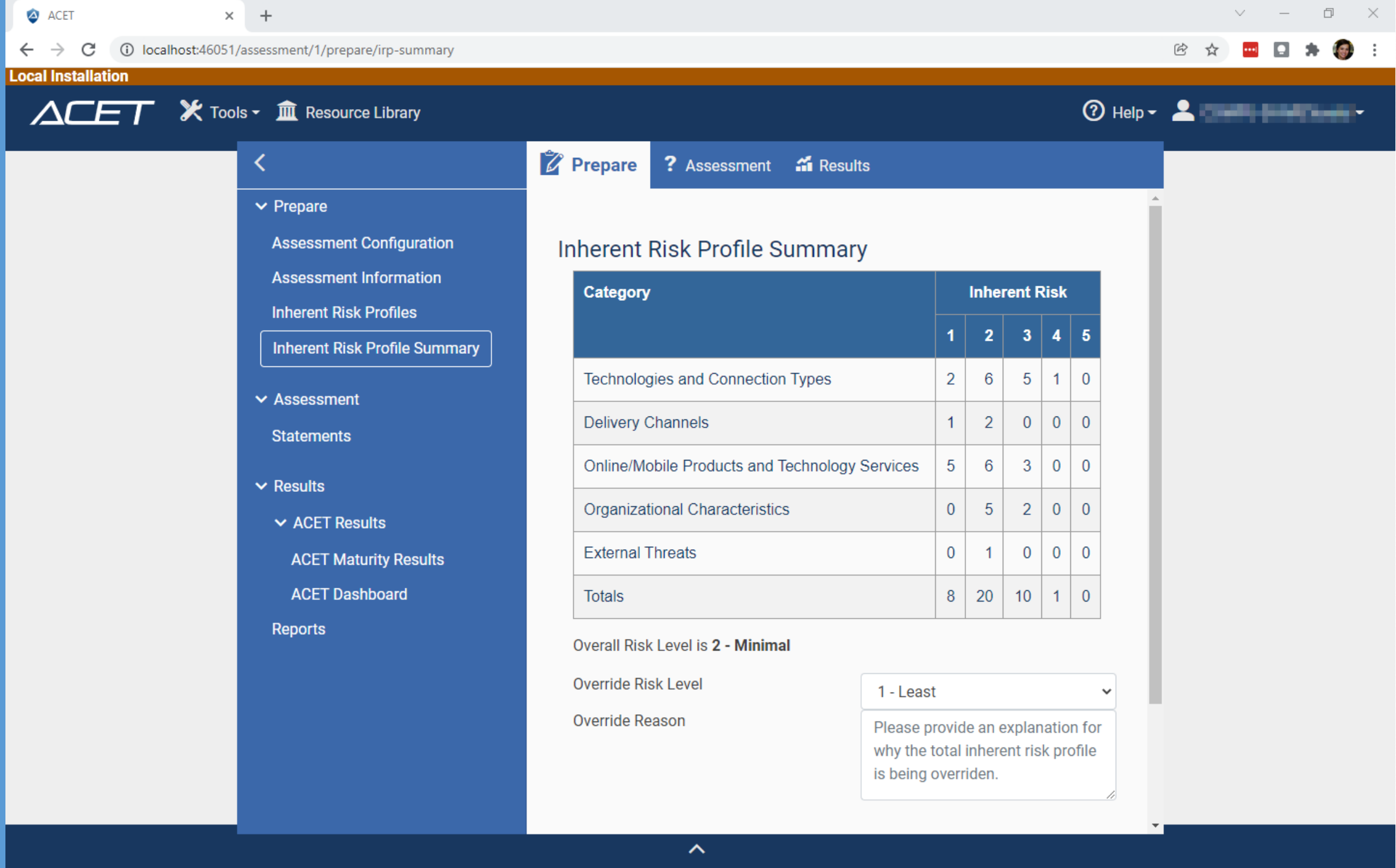
Tandem

Sample ACEvT Local App



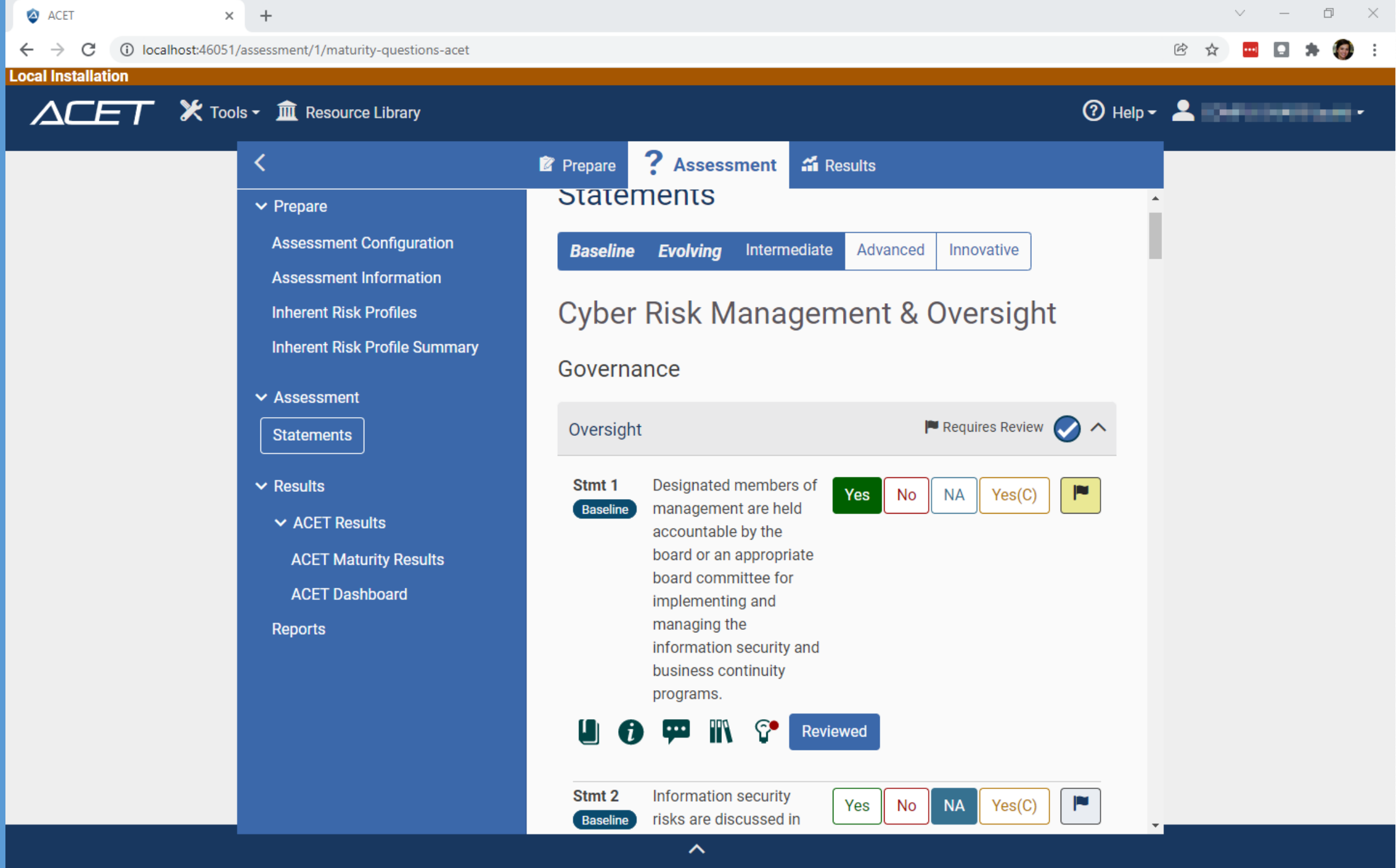
Tandem

Sample ACEvT Local App



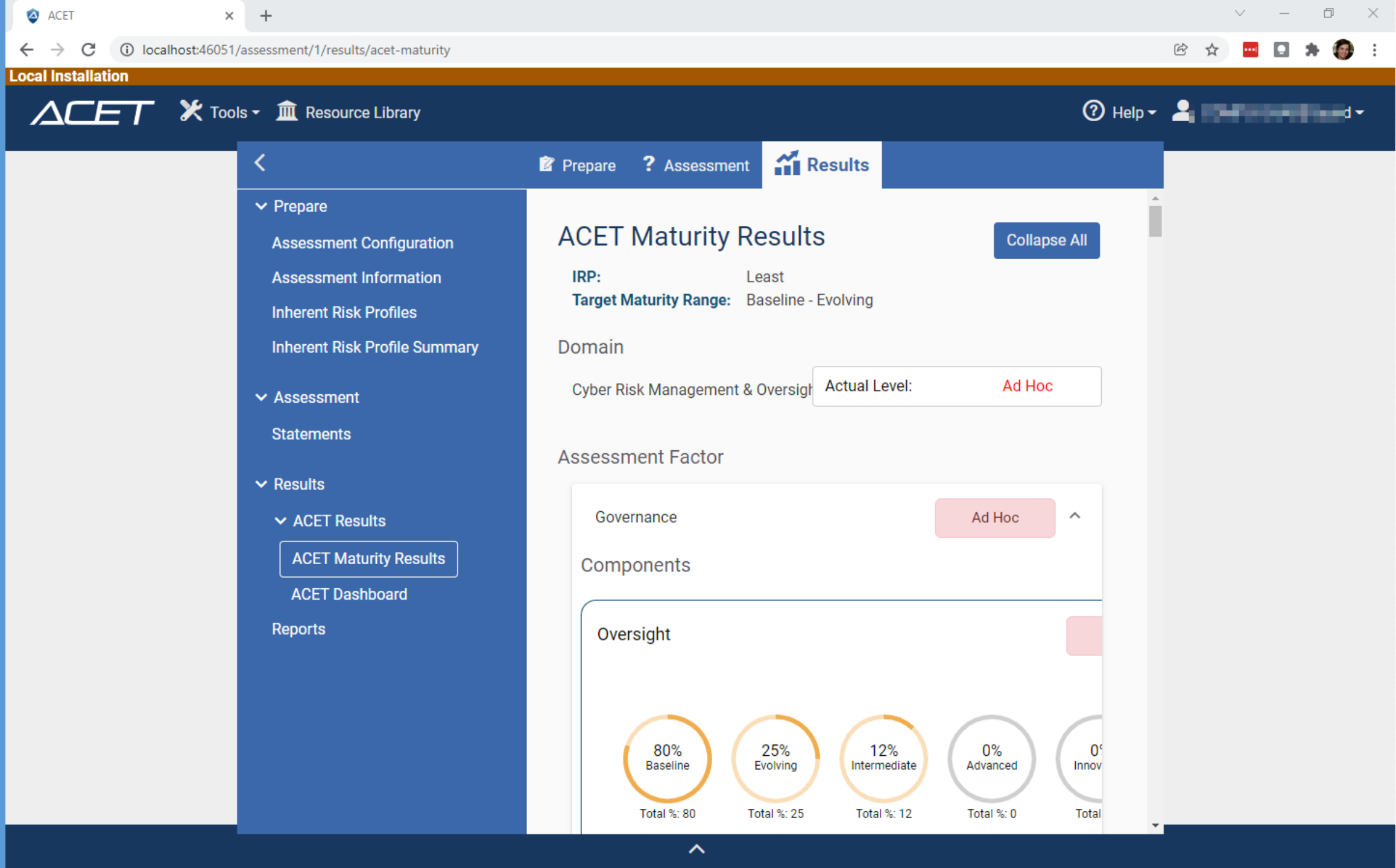
Tandem

Sample ACEvT Local App



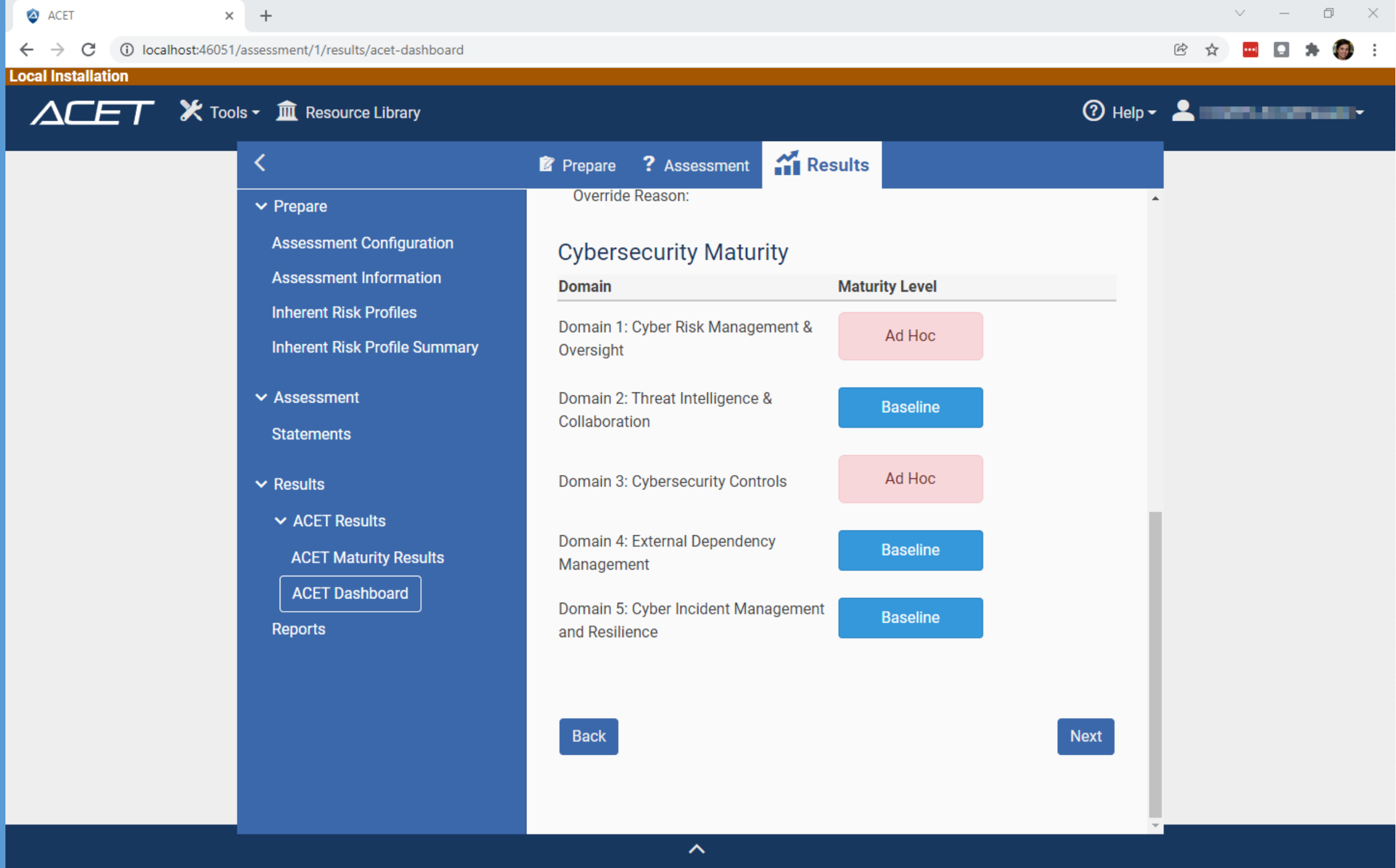
Tandem

Sample ACEvT Local App



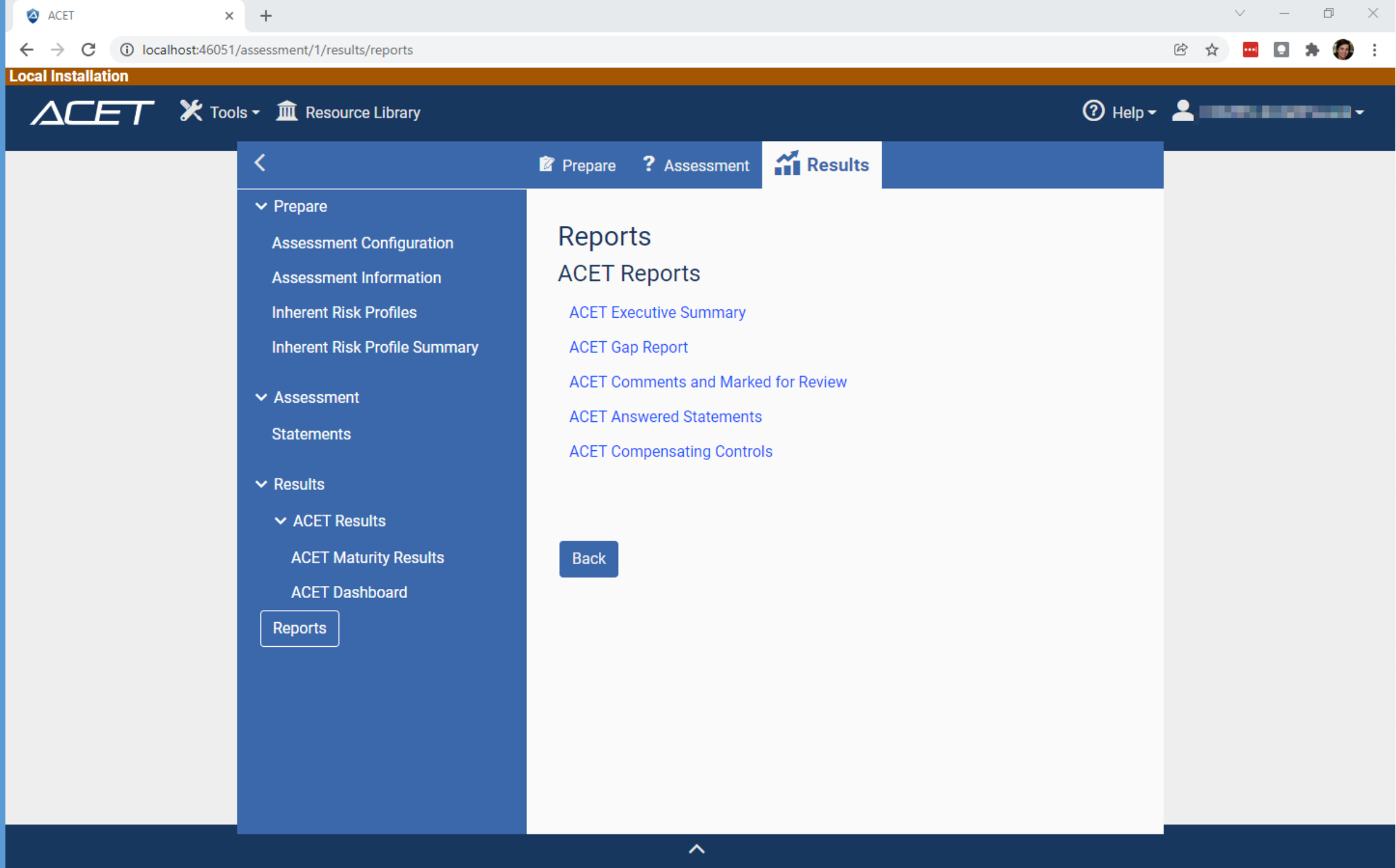
Tandem

Sample ACEvT Local App



Tandem

Sample ACEvT Local App



Tandem

Sample ACEvT Local App

ACET | Answered Statements Report - A

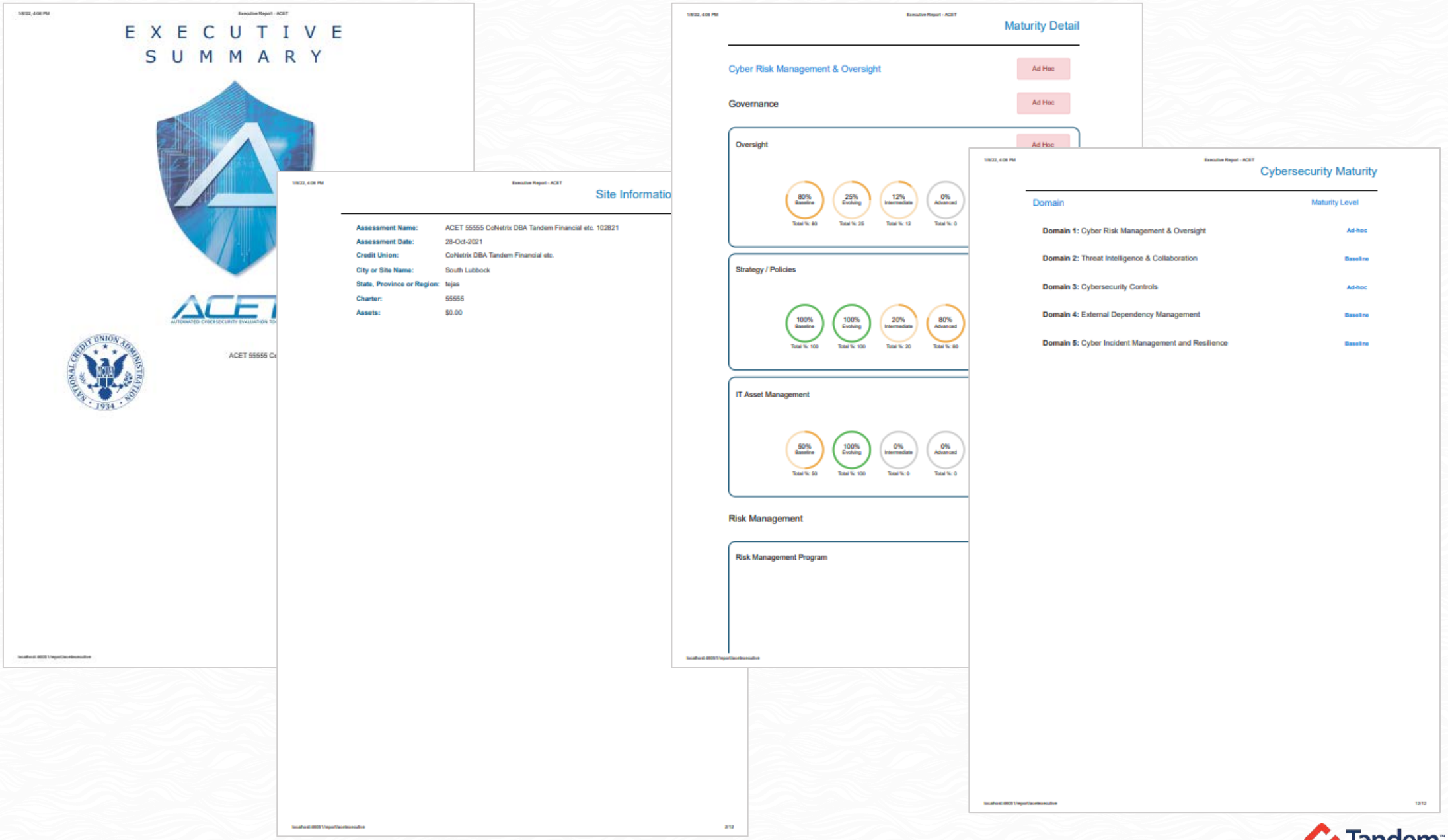
localhost:46051/report/acetansweredquestions

ANSWERED STATEMENTS REPORT

ACET
AUTOMATED CYBERSECURITY EVALUATION TOOLBOX

Tandem

Sample ACEvT Local App



Tandem

Sample ACEvT Local App

GAP REPORT

ACET

AUTOMATED CYBERSECURITY EVALUATION TOOLBOX

ACET 55555 CoNetrix DBA Tandem Financial etc. 102821

28-Oct-2021

Isaiid

$0.00

This gap report lists the statements that are answered "No".

This is often referred to as the GAP Report. This report intends to list the gaps, assist users of the report in identifying gaps, prioritizing work, and beginning to make a plan to address the gaps by implementing the controls.

The percentage gap in each domain is also listed and will help to determine the priority. ACET is a cumulative maturity model meaning lower levels should be completed before moving to higher levels. Ideally baseline should be completed before focusing efforts on controls in evolving and so forth up the line of maturity levels.

Gaps

Marked for Review -

Cyber Risk Management & Oversight - Domain

Governance - Assessment Factor

Oversight - Component

Stmt 4	The budgeting process includes information security related expenses and tools.	No
Stmt 6	At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.	No
Stmt 8	Cybersecurity tools and staff are requested through the budget process.	No
Stmt 9	There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.	No

IT Asset Management - Component

Stmt 48	Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.	No
Stmt 50	A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools.	No

Resources - Assessment Factor

Staffing - Component

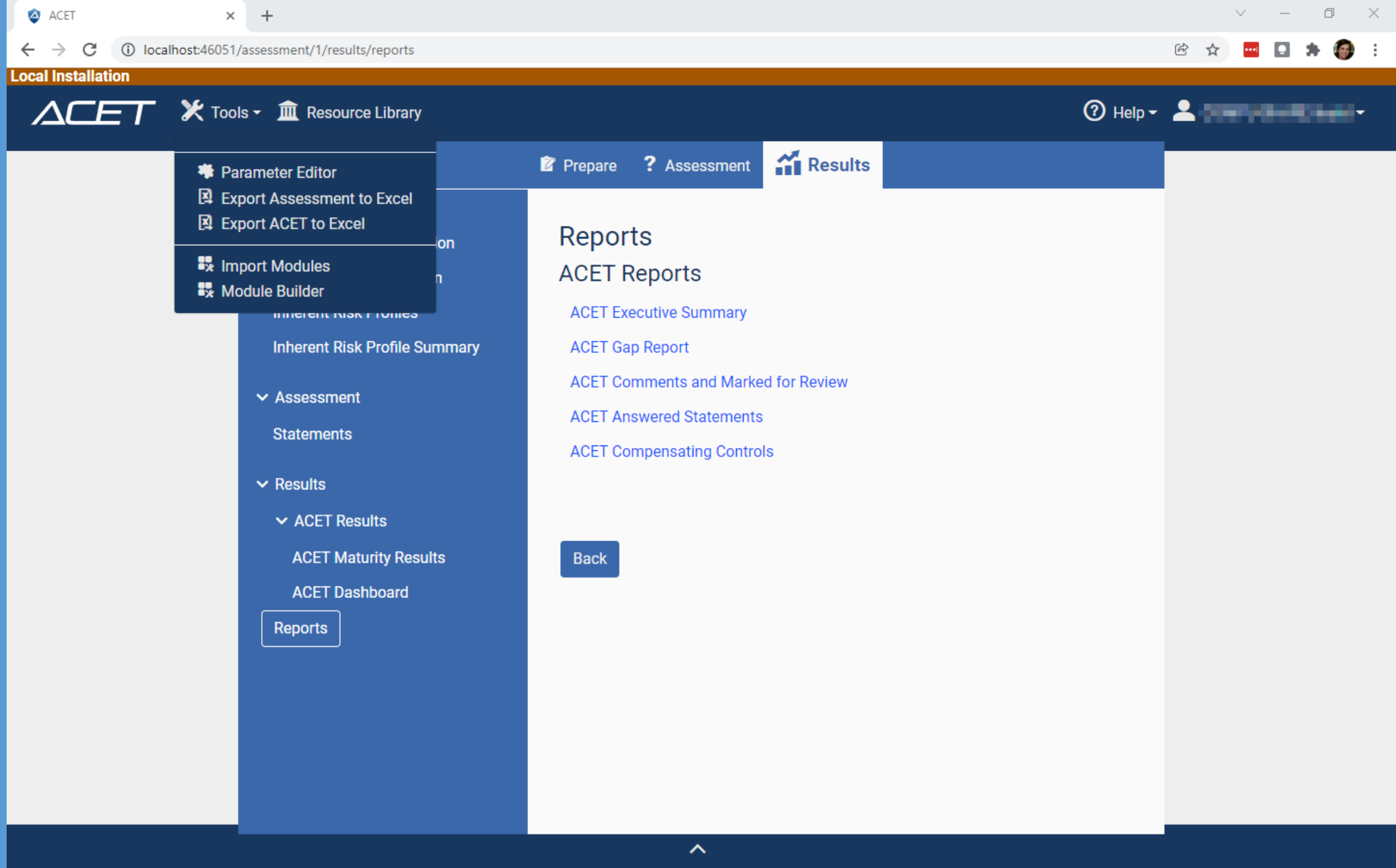
Stmt 111	Management with appropriate knowledge and experience leads the institution's cybersecurity efforts.	No
Stmt 113	Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.	No

Training and Culture - Assessment Factor

Training - Component

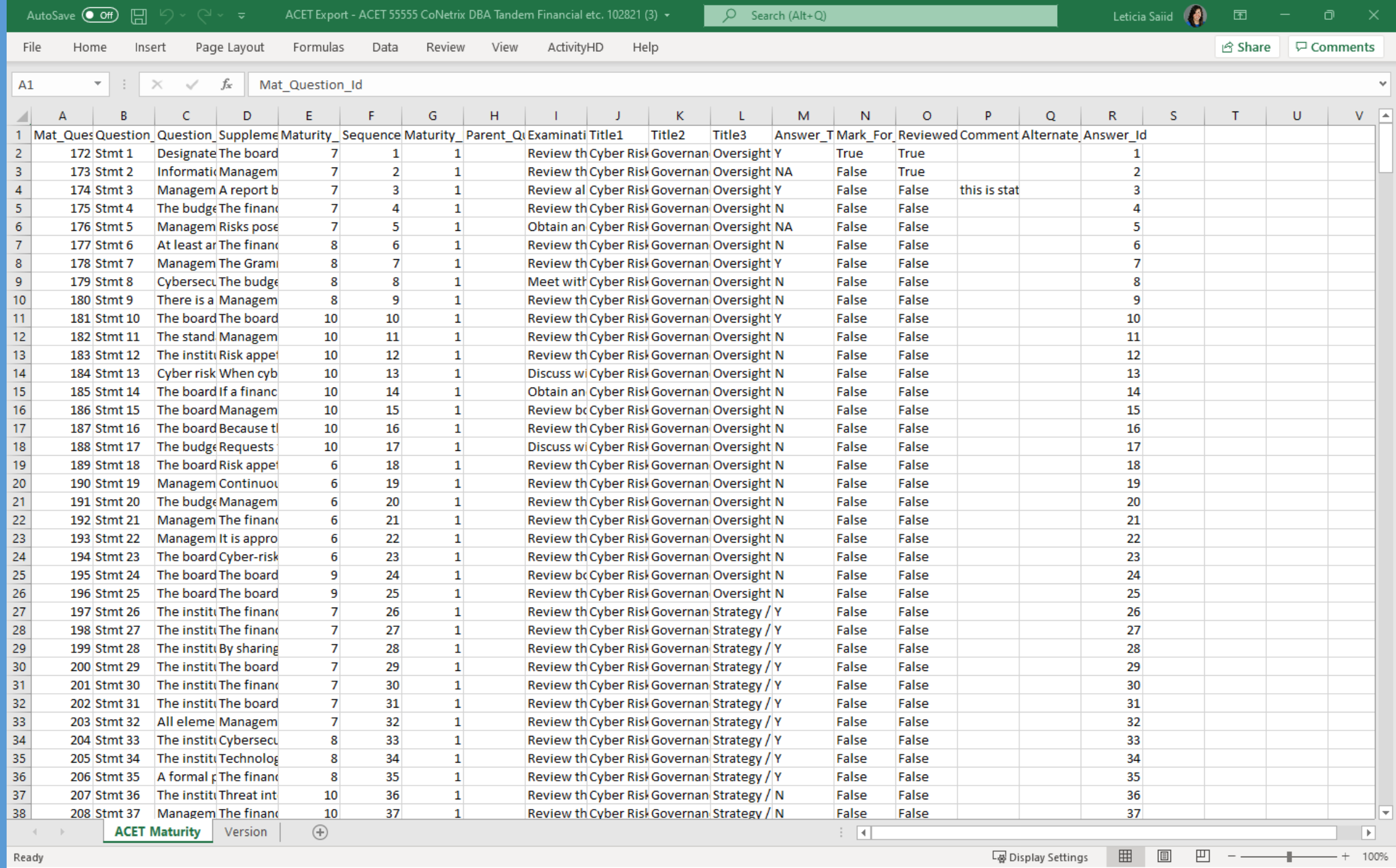
Tandem™

Sample ACEvT Local App



Tandem

Sample ACEvT Local App



AutoSave Off | ACET Export - ACET 55555 CoNetrix DBA Tandem Financial etc. 102821 (3) | Search (Alt+Q) | Leticia Saiid

File Home Insert Page Layout Formulas Data Review View ActivityHD Help | Share | Comments

A1 | Mat_Question_Id

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	Mat_Ques	Question_	Question_	Suppleme	Maturity_	Sequence	Maturity_	Parent_Q	Examinati	Title1	Title2	Title3	Answer_T	Mark_For_	Reviewed	Comment	Alternate_	Answer_Id				
2	172	Stmt 1	Designate	The board	7	1	1		Review th	Cyber Risk	Governan	Oversight	Y	True	True			1				
3	173	Stmt 2	Informatic	Managem	7	2	1		Review th	Cyber Risk	Governan	Oversight	NA	False	True			2				
4	174	Stmt 3	Managem	A report b	7	3	1		Review al	Cyber Risk	Governan	Oversight	Y	False	False	this is stat		3				
5	175	Stmt 4	The budge	The financ	7	4	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			4				
6	176	Stmt 5	Managem	Risks pose	7	5	1		Obtain an	Cyber Risk	Governan	Oversight	NA	False	False			5				
7	177	Stmt 6	At least ar	The financ	8	6	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			6				
8	178	Stmt 7	Managem	The Gramı	8	7	1		Review th	Cyber Risk	Governan	Oversight	Y	False	False			7				
9	179	Stmt 8	Cybersecu	The budge	8	8	1		Meet with	Cyber Risk	Governan	Oversight	N	False	False			8				
10	180	Stmt 9	There is a	Managem	8	9	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			9				
11	181	Stmt 10	The board	The board	10	10	1		Review th	Cyber Risk	Governan	Oversight	Y	False	False			10				
12	182	Stmt 11	The stand	Managem	10	11	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			11				
13	183	Stmt 12	The institu	Risk appet	10	12	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			12				
14	184	Stmt 13	Cyber risk	When cyb	10	13	1		Discuss wi	Cyber Risk	Governan	Oversight	N	False	False			13				
15	185	Stmt 14	The board	If a financ	10	14	1		Obtain an	Cyber Risk	Governan	Oversight	N	False	False			14				
16	186	Stmt 15	The board	Managem	10	15	1		Review bo	Cyber Risk	Governan	Oversight	N	False	False			15				
17	187	Stmt 16	The board	Because tl	10	16	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			16				
18	188	Stmt 17	The budge	Requests	10	17	1		Discuss wi	Cyber Risk	Governan	Oversight	N	False	False			17				
19	189	Stmt 18	The board	Risk appet	6	18	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			18				
20	190	Stmt 19	Managem	Continuou	6	19	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			19				
21	191	Stmt 20	The budge	Managem	6	20	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			20				
22	192	Stmt 21	Managem	The financ	6	21	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			21				
23	193	Stmt 22	Managem	It is appro	6	22	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			22				
24	194	Stmt 23	The board	Cyber-risk	6	23	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			23				
25	195	Stmt 24	The board	The board	9	24	1		Review bo	Cyber Risk	Governan	Oversight	N	False	False			24				
26	196	Stmt 25	The board	The board	9	25	1		Review th	Cyber Risk	Governan	Oversight	N	False	False			25				
27	197	Stmt 26	The institu	The financ	7	26	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			26				
28	198	Stmt 27	The institu	The financ	7	27	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			27				
29	199	Stmt 28	The institu	By sharing	7	28	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			28				
30	200	Stmt 29	The institu	The board	7	29	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			29				
31	201	Stmt 30	The institu	The financ	7	30	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			30				
32	202	Stmt 31	The institu	The board	7	31	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			31				
33	203	Stmt 32	All eleme	Managem	7	32	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			32				
34	204	Stmt 33	The institu	Cybersecu	8	33	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			33				
35	205	Stmt 34	The institu	Technolog	8	34	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			34				
36	206	Stmt 35	A formal p	The financ	8	35	1		Review th	Cyber Risk	Governan	Strategy /	Y	False	False			35				
37	207	Stmt 36	The institu	Threat int	10	36	1		Review th	Cyber Risk	Governan	Strategy /	N	False	False			36				
38	208	Stmt 37	Managem	The financ	10	37	1		Review th	Cyber Risk	Governan	Strategy /	N	False	False			37				

ACET Maturity | Version

Ready | Display Settings | 100%

Tandem

Sample Tandem Cybersecurity

Maturity | Tandem

secure.tandem.app/SelfAssessments/Maturity?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

Cybersecurity

Tandem Financial
Lubbock, TX

Global | July 2021 | + Open

- Dashboard
- Request List
- Inherent Risk
- Maturity
- Analysis
  - Gap Analysis
- Peer Analysis
- Reports
- Revision/Approval Log
- Download Documents

- Knowledge Base
- Settings

Maturity Levels

Notify Cybersecurity Users

Domain	Completed	Maturity Level
Cyber Risk Management and Oversight	141/141	Baseline
Threat Intelligence and Collaboration	45/45	Evolving
Cybersecurity Controls	174/174	Evolving
External Dependency Management	51/51	Evolving
Cyber Incident Management and Resilience	83/83	Intermediate

Tandem

Tandem © 2022 Tandem

Sample Tandem Cybersecurity

Tandem

Cybersecurity Maturity: Cyber Ris

secure.tandem.app/SelfAssessments/MaturityQuestionnaire?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339&componentId=1

- Peer Analysis
- Reports
- Revision/Approval Log
- Download Documents
- Knowledge Base
- Settings

Governance: Governance includes oversight, strategies, policies, and IT asset management to implement an effective governance of the cybersecurity program.

Responsible

	Type	Name
	Employee	Jill Sanderson

+ Responsibility

View Only Unanswered Questions

View Only Flagged Questions

BASELINE

1. Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.

- (•) Yes
- ( ) Yes with Compensating Controls
- ( ) No

Comments (1) | Responsible (2) | Attachments (1) | References

2. Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.

- (•) Yes
- ( ) Yes with Compensating Controls
- ( ) No

Comments (0) | Responsible (0) | Attachments (0) | References

3. Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.

Save | Save & Go to Next | Cancel | Maturity: Baseline | Next: Strategy / Policies

Sample Tandem Cybersecurity

Analysis July 2021 | Tandem

secure.tandem.app/SelfAssessments/Analysis?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

- Dashboard
- Request List
- Inherent Risk
- Maturity
- Analysis
  - Gap Analysis
- Peer Analysis
- Reports
- Revision/Approval Log
- Download Documents
- Knowledge Base
- Settings

Analysis

The mapping below identifies where each *Cybersecurity Maturity* domain exists in relation to your *Inherent Risk Profile*. FFIEC guidance recommends results should fall within the sections marked in blue. Any domains with a Sub-Baseline rating should be addressed immediately. Mark the **Show target risk/maturity levels** to also see the target results on the chart.

☑ Show target risk/maturity levels

Cybersecurity Maturity	Inherent Risk: Least	Minimal	Moderate	Significant	Most
Innovative					
Advanced					
Intermediate			Cyber Incident Management and Resilience		
Evolving		Cyber Risk Management and Oversight Threat Intelligence and Collaboration Cybersecurity Controls External Dependency Management Cyber Incident Management and Resilience	Threat Intelligence and Collaboration Cybersecurity Controls External Dependency Management		
Baseline			Cyber Risk Management and Oversight		

Tandem © 2022 Tandem

Sample Tandem Cybersecurity

Gap Analysis July 2021 | Tandem

secure.tandem.app/SelfAssessments/GapAnalysis?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

Cybersecurity

Tandem Financial
Lubbock, TX

Global | July 2021 | + Open

- Dashboard
- Request List
- Inherent Risk
- Maturity
- Analysis
- Gap Analysis
- Peer Analysis
- Reports
- Revision/Approval Log
- Download Documents
- Knowledge Base
- Settings

Gap Analysis

Inherent Risk

	Risk Level	Target
Overall	Moderate	Minimal

Cybersecurity Maturity

Download plan for improving maturity level to: Evolving

Domain	Maturity Level	Target	Recommended	
Cyber Risk Management and Oversight	Baseline	Evolving	Evolving	⚠
Threat Intelligence and Collaboration	Evolving	Evolving		✓
Cybersecurity Controls	Evolving	Evolving		✓
External Dependency Management	Evolving	Evolving		✓
Cyber Incident Management and Resilience	Intermediate	Evolving		✓

Tandem

Tandem © 2022 Tandem

Sample Tandem Cybersecurity

Gap Analysis: Cyber Risk Manage

secure.tandem.app/SelfAssessments/MaturityGapAnalysis?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339&domainId=1

Cybersecurity

Tandem Financial
Lubbock, TX

Global | July 2021 × | + Open

- Dashboard
- Request List
- Inherent Risk
- Maturity
- Analysis
  - Gap Analysis
- Peer Analysis
- Reports
- Revision/Approval Log
- Download Documents
- Knowledge Base
- Settings

Gap Analysis: Cyber Risk Management and Oversight

Show plan for improving maturity level to: Evolving

Domain	Maturity Level	Target	Recommended
Cyber Risk Management and Oversight	Baseline	Evolving	Evolving
Governance			
Oversight	Baseline	Evolving	Evolving

Plan of Action

To improve to Evolving

1. Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.

+ Create Task | Edit Answer

← Previous | Next → | Jump to:

Tandem © 2022 Tandem

Tandem

Sample Tandem Cybersecurity

Tandem

Peer Analysis July 2021 | Tandem

secure.tandem.app/SelfAssessments/PeerAnalysis?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

Cybersecurity

Tandem Financial
Lubbock, TX

Global | July 2021 | + Open

- Dashboard
- Request List
- Inherent Risk
- Maturity
- Analysis
  - Gap Analysis
  - Peer Analysis
  - Reports
  - Revision/Approval Log
  - Download Documents
- Knowledge Base
- Settings

Peer Analysis

The mapping below represents the risk and maturity of other financial institutions. Data was pulled and anonymized from the most current completed assessment of institutions that have opted in to **Peer Analysis**. A total of **768** completed assessments are included in the data set.

Regulatory Body: -All-

Asset Size: -All-

Filter Results

Risk/Maturity

Cybersecurity Domain: Overall

Maturity	Inherent Risk: Least	Minimal	Moderate	Significant	Most
Innovative	*0.13%*	*0.26%*	*0.00%*	*0.00%*	*0.00%*
Advanced	*0.13%*	*0.00%*	*0.00%*	*0.00%*	*0.00%*
Intermediate	*0.39%*	*2.21%*	*0.13%*	*0.00%*	*0.00%*

Sample Tandem Cybersecurity

Cybersecurity Maturity	Inherent Risk: Least	Minimal	Moderate	Significant	Most
Innovative	0.13%	0.26%	0.00%	0.00%	0.00%
Advanced	0.13%	0.00%	0.00%	0.00%	0.00%
Intermediate	0.39%	2.21%	0.13%	0.00%	0.00%
Evolving	0.39%	13.02%	1.30%	0.13%	0.00%
Baseline	9.90%	62.50%	2.73%	0.00%	0.00%
Sub-Baseline	0.26%	6.12%	0.39%	0.00%	0.00%

Inherent Risk

Category	Risk Level	Average Answer	Average Peer Risk
Technologies and Connection Types	Minimal	Minimal (1.50)	Minimal (1.28)
Delivery Channels	Most	Most (4.17)	Moderate (2.70)
Online/Mobile Products and Technology Services	Moderate	Moderate (2.64)	Minimal (1.23)
Organizational Characteristics	Significant	Minimal (1.93)	Least (1.00)
External Threats	Least	Least (0.50)	Minimal (1.61)
Overall	**Moderate**	**Moderate (2.17)**	**Moderate (2.50)**

Tandem

Sample Tandem Cybersecurity

Tandem

Peer Analysis July 2021 | Tandem

secure.tandem.app/SelfAssessments/PeerAnalysis?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

Cybersecurity Maturity

Domain	Maturity Level	Average Peer Maturity
Cyber Risk Management and Oversight	Baseline	Baseline (0.93)
Governance		
Oversight	Baseline	Evolving (1.69)
Strategy / Policies	Intermediate	Evolving (1.74)
IT Asset Management	Intermediate	Evolving (1.78)
Risk Management		
Risk Management Program	Innovative	Evolving (1.68)
Risk Assessment	Advanced	Intermediate (2.45)
Audit	Intermediate	Evolving (1.93)
Resources		
Staffing	Intermediate	Evolving (1.77)
Training and Culture		
Training	Intermediate	Evolving (1.75)
Culture	Intermediate	Intermediate (2.03)
Threat Intelligence and Collaboration	Evolving	Evolving (1.14)
Cybersecurity Controls	Evolving	Baseline (0.67)
External Dependency Management	Evolving	Baseline (0.96)
Cyber Incident Management and Resilience	Intermediate	Baseline (0.98)

Sample Tandem Cybersecurity

Tandem

Peer Cybersecurity Maturity: Cyb

secure.tandem.app/SelfAssessments/PeerMaturity?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339&componentId=1

Download Documents

Knowledge Base

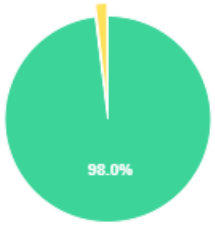
Settings

BASELINE

1. **Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.**

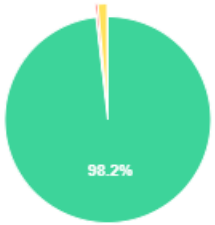
- Yes **98.05%**
- Yes with Compensating Controls **1.82%**
- No **0.13%**

See the attached meeting minutes for additional information about the expectations of the Board.



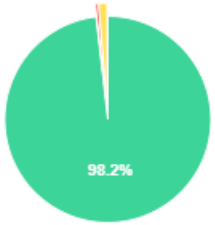
2. **Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.**

- Yes **98.18%**
- Yes with Compensating Controls **1.43%**
- No **0.39%**



3. **Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.**

- Yes **98.18%**
- Yes with Compensating Controls **1.30%**
- No **0.52%**



includes information security related expenses and tools.

Yes 97.01%

Previous Next

Sample Tandem Cybersecurity

Reports: July 2021 | Tandem

secure.tandem.app/SelfAssessments/Reports?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

Cybersecurity

Tandem Financial
Lubbock, TX

Global | July 2021 | + Open

- Dashboard
- Request List
- Inherent Risk
- Maturity
- Analysis
  - Gap Analysis
- Peer Analysis
- Reports
- Revision/Approval Log
- Download Documents

- Knowledge Base
- Settings

Reports

- Tasks
- Flagged Inherent Risk Profile Questions
- Flagged Cybersecurity Maturity Questions
- Flagged Request List Items
- Unanswered Inherent Risk Profile Questions
- Unanswered Cybersecurity Maturity Questions
- Request List Items Without a Response
- Responsibility

Tandem

Tandem

© 2022 Tandem

Sample Tandem Cybersecurity

Responsibility: July 2021 | Tander

secure.tandem.app/SelfAssessments/Responsibility?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

Global | July 2021 | + Open

- Dashboard
- Request List
- Inherent Risk
- Maturity
- Analysis
  - Gap Analysis
- Peer Analysis
- Reports
- Revision/Approval Log
- Download Documents
- Knowledge Base
- Settings

Responsibility

All Reports

Responsible

-All-

Only show users with unanswered questions

Search

Notify Cybersecurity Users

Displaying 1 - 12 of 12

< Previous **1** Next >

Assigned To	Category / Component	# Assigned	# Unanswered
Jill Sanderson	Delivery Channels	3	0
Assistant Compliance Officer	Technologies and Connection Types	1	0
Ed Smith	Technologies and Connection Types	1	0
Brady Cook	Delivery Channels	1	0
Jill Sanderson	Oversight	25	0
Information Security Committee	Oversight	1	0
Sam Westly ⚠	Oversight	1	0
Assistant ⚠	Threat Intelligence & Information	1	0
Austin Lee	Appendixes A and B to Part 748	1	0

Tandem

Sample Tandem Cybersecurity

Tandem

Download Documents - July 202

secure.tandem.app/SelfAssessments/Documents?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

Cybersecurity

Tandem Financial
Lubbock, TX

Global | July 2021 | + Open

- Dashboard
- Request List
- Inherent Risk
- Maturity
- Analysis
  - Gap Analysis
- Peer Analysis
- Reports
- Revision/Approval Log
- Download Documents
- Knowledge Base
- Settings

Download Documents

Cybersecurity Assessment

This document is designed to export this cybersecurity assessment's definitions, *Inherent Risk Profile* questions and answers, *Cybersecurity Maturity* questions and answers, and analysis of results in a printable format.

ACET

The completed cybersecurity assessment in the NCUA ACET (Automated Cybersecurity Examination Tool) format.

Cybersecurity Assessment Version Comparison

This document compares the current assessment to another completed assessment.

Assessment To Compare

December 2020

Report to the Board

Sample Tandem Cybersecurity

Tandem

Download Documents - July 202

secure.tandem.app/SelfAssessments/Documents?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

Report to the Board

This document is designed for presenting the board with responsibilities, definitions, results from the assessment, analysis of results, and questions to assist management and the board when reviewing results. Use the filters to display modified peer data in the document. If you do not use the filters, the document will show results from the full data set.

Regulatory Body

-All-

Asset Size

-All-

Gap Analysis

This document is designed for downloading a gap analysis to show plans for improving all cybersecurity maturity domains to the identified level.

Download plan for improving maturity level to Evolving

Request List Items

This document contains the *Request List* category, description, response, attachment status, and the name of the person that provided the response.

Include attachments

Inherent Risk Profile Questions

Sample Tandem Cybersecurity

Download Documents - July 202

secure.tandem.app/SelfAssessments/Documents?id=c610c5f6-1a6f-4eea-a2bb-ad2500e9a339

provided the response.

Include attachments

Inherent Risk Profile Questions

This document contains the *Inherent Risk Profile* category, question, answer, risk level, and the name of the person that provided the answer.

Include attachments

Cybersecurity Maturity Questions

This document contains the *Cybersecurity Maturity* domain, assessment factor, component, question, answer, maturity level, and the name of the person that provided the answer.

Include attachments

Peer Analysis

These documents show how frequently an answer was selected by organizations participating in the anonymous data set.

- (●) Inherent Risk Profile Peer Analysis
- ( ) Cybersecurity Maturity Peer Analysis

Regulatory Body

-All-

Asset Size

-All-

Tandem

Tandem

© 2022 Tandem

Sample Tandem Cybersecurity

TANDEM FINANC

Cybersecurity Assessment Report to Board of Directors

Tandem Financial

July 2021

Revision 1.3

Last Approved: 07/20/2021

3 Cybersecurity Maturity

The *Cybersecurity Maturity* levels below were determined for Tandem Financial by answ
statements organized into five domains taken from the FFIEC Cybersecurity Assessment
statement describes activities supporting assessment factors for each domain. To reach
domain, all declarative statements in that maturity level as well as previous maturity level
attained, but also sustained.

Cyber Risk Management and Oversight (D1)

Cyber risk management and oversight addresses the board of directors' (board's) oversig
development and implementation of an effective enterprise-wide cybersecurity program w
policies and procedures for establishing appropriate accountability and oversight.

Target Maturity	Recommended Maturity	Maturity
Evolving	Evolving	Baseline

**The peer maturity for a domain is calculated by averaging the domain ratings from peers
calculated by averaging the peer maturity of each component (below), it is possible for th
domain level to be lower than the peer maturity of all of its components.*

Components

Component	Maturity Level
Risk Management Program	Innovative
Risk Assessment	Advanced
Audit	Intermediate
Culture	Intermediate
IT Asset Management	Intermediate
Staffing	Intermediate
Strategy / Policies	Intermediate
Training	Intermediate
Oversight	Baseline

Copyright © 2022 Confidential - Internal Use Only Generated by Tandem

4 Analysis

The table below depicts the relationship between the Inherent Risk Profile and the domain maturity levels (D1, D2, etc.) calculated by the assessment for Tandem Financial as well as the target levels (T1, T2, etc.) determined by management. Domain maturity is located under the assessment inherent risk column of Moderate, based on the institution's overall inherent risk level. Guidance recommends domain maturity fall within the sections marked in blue. Any domain with a rating of Sub-Baseline should be addressed immediately.

Cybersecurity Maturity	Inherent Risk: Least	Minimal	Moderate	Significant	Most
Innovative					
Advanced					
Intermediate			D5		
Evolving		T1, T2, T3, T4, T5	D2, D3, D4		
Baseline			D1		
Sub-Baseline					

Recommended Remediation

The following declarative statements were marked as "No" in the assessment causing domain maturity levels to fall below the assessment recommended maturity level. In order for Tandem Financial to achieve the FFIEC recommended maturity level in each domain, each of the following declarative statements must be marked as "Yes."

- Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.

Copyright © 2022 Confidential - Internal Use Only Generated by Tandem

Tandem

Sample Tandem Cybersecurity

TANDEM FINANCIAL

Cybersecurity Assess
Version Comparison

Tandem Financial

July 2021 vs. December 2020

Table of Contents

2 Inherent Risk Profile

Inherent risk incorporates the type, volume, and
threats directed at the institution Inherent risk ca
controls. The inherent risk below was calculated
FFIEC Cybersecurity Assessment Tool. Each qu
FFIEC. Risk level definitions have been included

Overall Inherent Risk

	December 2020	July
Identified Risk	Moderate	Mode
Target Risk	Minimal	Mini

Inherent Risk by Category

Category
Technologies and Connection Types

Certain types of connections and technologies
inherent risk depending on the complexity and
and nature of the specific technology products
category includes the number of Internet servic
third-party connections, whether systems are h
outsourced, the number of unsecured connecti
access, volume of network devices, end-of-life
services, and use of personal devices.

Copyright © 2022 Confidential - Internal Use Only Generated by Tandem

3 Cybersecurity Maturity

The *Cybersecurity Maturity* levels below were determined for Tandem Financial by answering 494 declarative statements organized into five domains taken from the FFIEC Cybersecurity Assessment Tool. Each declarative statement describes activities supporting assessment factors for each domain. To reach a maturity level in a domain, all declarative statements in that maturity level as well as previous maturity levels must not only be attained, but also sustained.

Cyber Risk Management and Oversight

Cyber risk management and oversight addresses the board of directors' (board's) oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.

December 2020	July 2021	Target	Recommended
Baseline	Baseline	Evolving	Evolving

Components

Component	December 2020	July 2021
Oversight	Baseline	Baseline
Risk Management Program	Innovative	Innovative
Staffing	Intermediate	Intermediate
Training	Intermediate	Intermediate
Strategy / Policies	Intermediate	Intermediate
Risk Assessment	Advanced	Advanced
Culture	Intermediate	Intermediate
IT Asset Management	Intermediate	Intermediate
Audit	Intermediate	Intermediate

Threat Intelligence and Collaboration

Threat intelligence and collaboration includes processes to effectively discover, analyze, and understand cyber threats, with the capability to share information internally and with appropriate third parties.

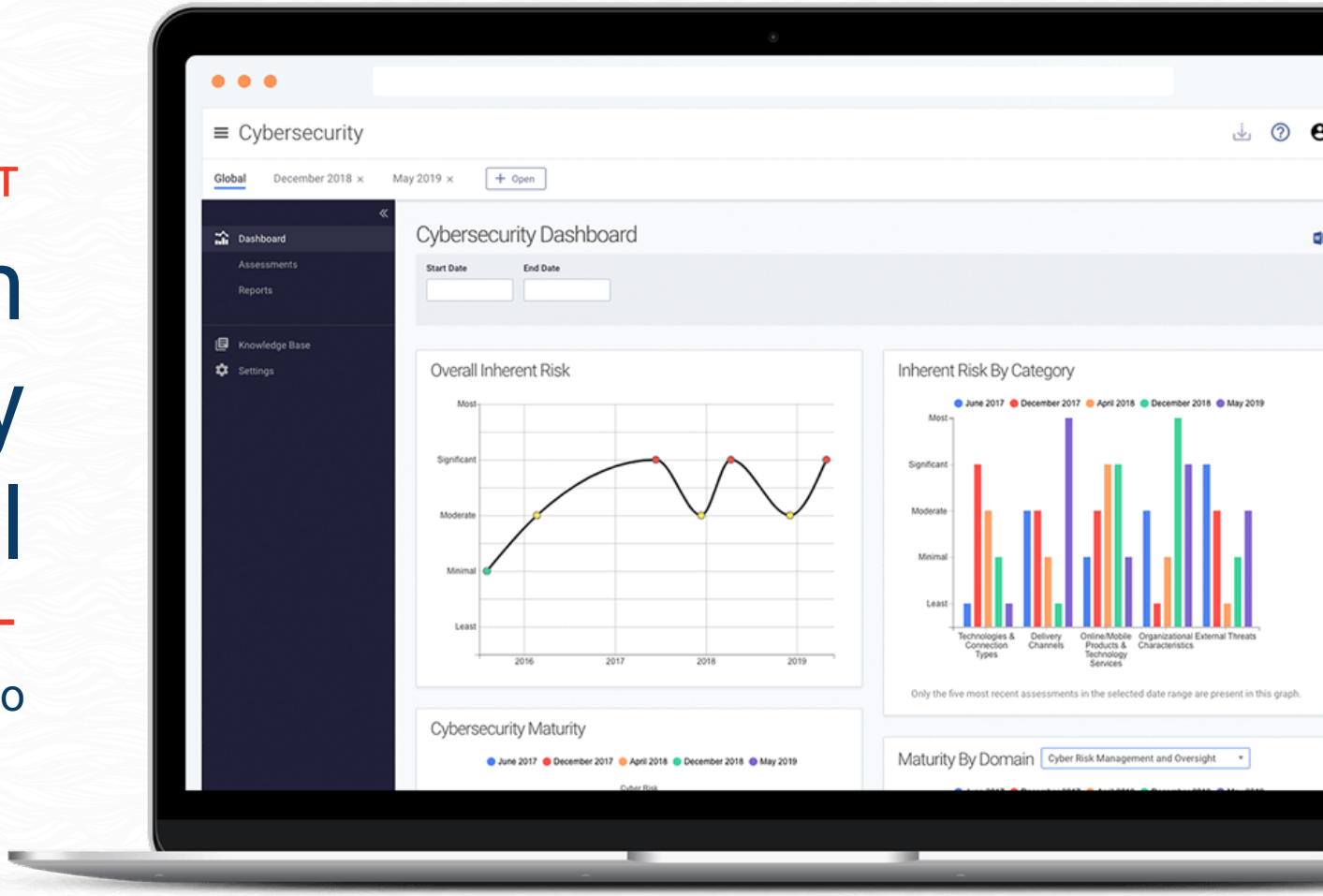
Copyright © 2022 Confidential - Internal Use Only Generated by Tandem

Tandem

WATCH A VIDEO ABOUT

Tandem Cybersecurity Assessment Tool

https://tandem.app/2022-cybersecurity-demo



Tandem

Tandem

THANKS FOR JOINING

What the New ACET Means for Your Next IT Exam

Leticia Saiid, Security+
Chief of Staff
Tandem, LLC

https://www.linkedin.com/in/leticiasaiid/
https://tandem.app/speakers/leticia-saiid

Tandem

Q&A