FFIEC Cybersecurity Assessment Tool
Automated Scoring Using an Excel Workbook

User Guide | Version 3.3.1 | October 1, 2019

WATKINS CONSULTING

839 Bestgate Road #400
Annapolis, MD 21401

www.watkinsconsulting.com

Summary

This is a user guide for the Excel tool created to automate answer tracking and scoring for the June 2015 *Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (Update May 2017)* [1]. The purpose of the cybersecurity assessment tool is described in the *FFIEC Cybersecurity Assessment Tool Overview for Chief Executive Officers and Boards of Directors* [2]. This user guide assumes that those documents are used to determine the appropriate use of this tool. This user guide only details how to use the Excel workbook.

If you need help with using the tool or interpreting the results, Watkins Consulting can help with interpreting and applying the FFIEC guidelines, cybersecurity governance issues and a wide range of other cybersecurity issues, including breach remediation and penetration testing

What Is New?

Watkins Excel Workbook—More Flexibility

We have listened to your suggestions. Beyond some formatting changes here are the changes from earlier workbooks.

- Version 2.1 and 3.3
  - Added four worksheets
    - Table of Contents (TOC)—designed to help navigate between the twenty worksheets
    - Appendix A—added the May 2017 version 1.1 text to make it easier to access the reference material associated with the declarative statements
    - Pivot Reports—build your own reports (unprotected)
    - Table Roll Up—all risk maturity domains combined into one Excel table
  - Added warning message if an entire component is marked as "N/A" (for fix, see page 5).
- Version 1.02 and 2.1
  - Firm name and report date are added to all worksheets.
  - Added controlled risk indicator "Yes(C)" for risk maturity declarative statements.
  - Added log worksheet.

Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved

- Broke up an unintentionally grouped declarative statements (Risk Management/Training and Culture/Culture/Evolving).

Risk Management and Oversight

This last change is the only item which will keep you from directly cutting and pasting from your current workbook to the revised workbook. So just be careful when cutting and pasting to the **Risk Management and Oversight Risk Maturity** worksheet. Where you had one answer before, you will need to expand the *Training and Culture/Culture/Evolving* to three.

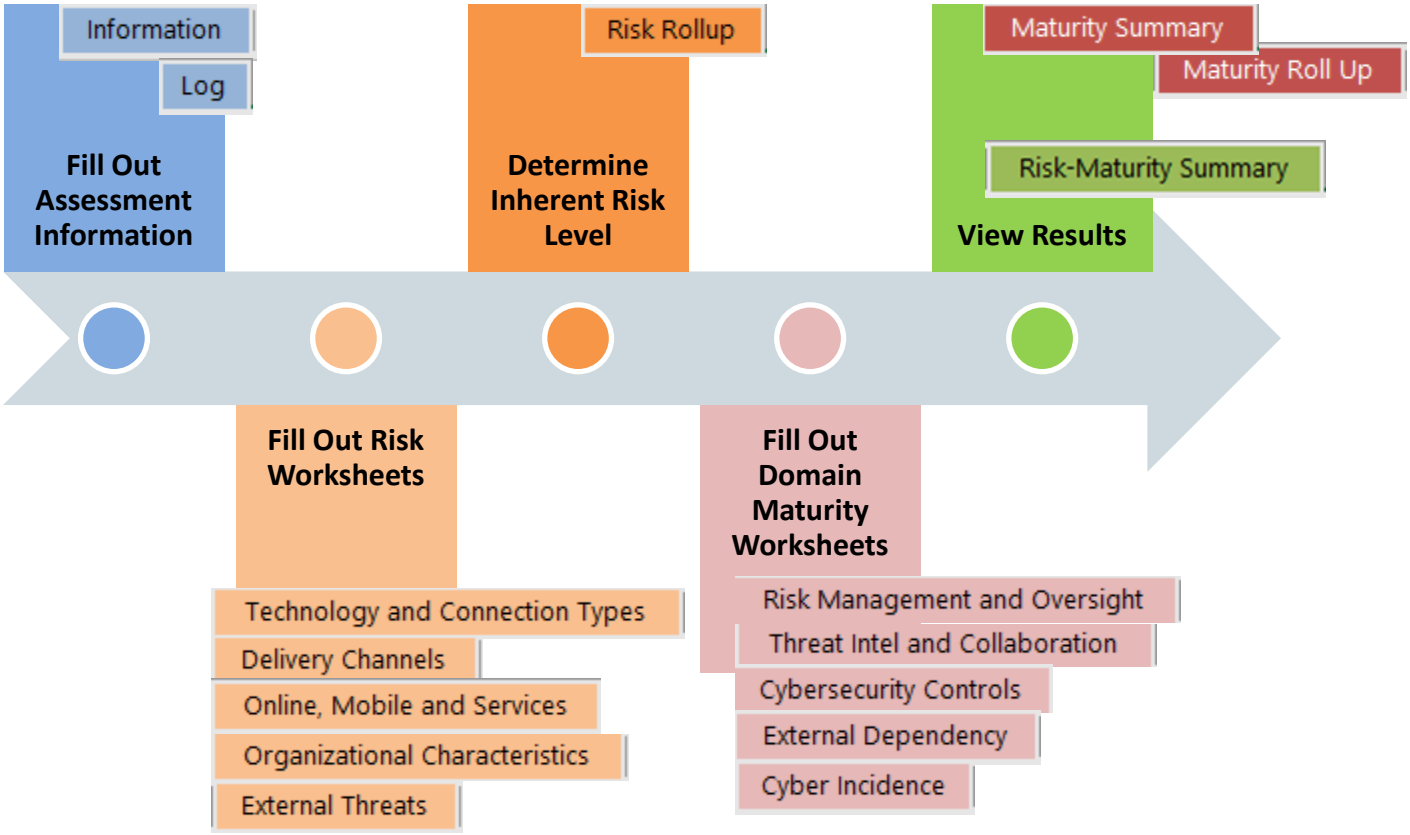
Obtain

The Excel workbook is available from the Watkins Consulting website, https://watkinsconsulting.com/our-projects/ffiec-cybersecurity-assessment-tool.

Overview

The task has been broken down into a workflow based on the CAT elements, as depicted below. You can complete your assessment by filling out the following: the information worksheet, the five risk worksheets, the inherent risk level worksheet, the domain maturity worksheets, and then selecting how to display the results on the risk-maturity summary.

Additional review and analysis can be accomplished with the risk maturity summary, the risk roll up, the table roll up and the pivot table worksheets.



Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved

Organization Details

The workbook closely follows the FFIEC approach. The tool is split up into 20 worksheets. Each worksheet is described below.

Information

Information: contact, version and copyright information.

- We recommend that you use the link in cell `A8` to send us your email so that we can notify you of updates. We will not share your information, per our on-line privacy policy [3].
- **Recommended Inputs**: Firm name (cell `B18`) and date (cell `B19`). These will be shown on the other worksheets for reference.
- **Optional Inputs**: Assessor (cell `B20`) and general notes (cell `B21`).

Log

Optionally keep track of your workflow on the **Log** worksheet.

TOC

Table of contents, **TOC**, eases navigation between the 20 worksheets. We recommend adding the "Back" and "Forward" buttons to the quick access toolbar as well.

Risk-Maturity Summary

Risk-Maturity Summary (green tab): this is an output populated from the inherent risk rollup and domain maturity sections.

- The only option is in cell `I15` which allows you to select how the domains will be displayed on the matrix—by name (default) or by number.
-

Risk Rollup

Risk Rollup (orange tab): this summarizes the inherent risks associated with each risk category.

- **Required Input:** Overall inherent risk level (cell `C17`). Once you have completed answering the questions in the risk category worksheets, the scoring for each category will be shown above this input. Your firm should use its judgement about risk to determine the appropriate risk level (least, minimal, moderate, significant, most), per the Cybersecurity Assessment Tool, page 4:

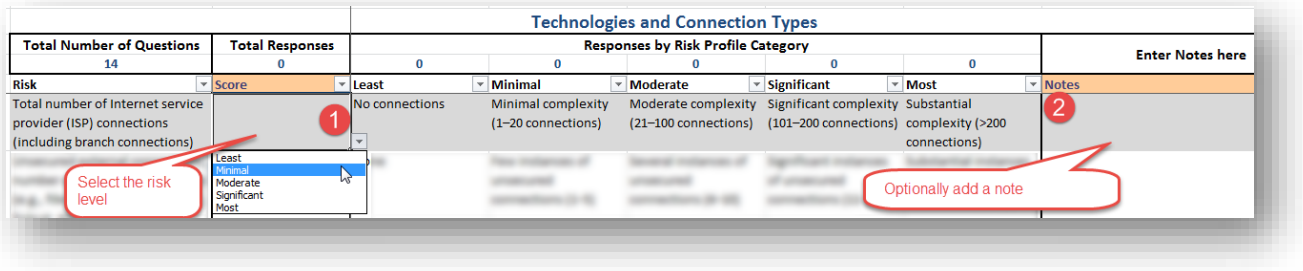
> *Determine Inherent Risk Profile*
>
> *Management can determine the institution's overall Inherent Risk Profile based on the number of applicable statements in each risk level for all activities (Figure 2). For example, when a majority of activities, products, or services fall within the Moderate Risk Level, management may determine that the institution has a Moderate Inherent Risk Profile. Each category may, however, pose a different level of inherent risk. Therefore, in addition to evaluating the number of instances that an institution selects for a specific risk level, management may also consider evaluating whether the specific category poses additional risk. [1]*

Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved

Technology and Connection Types | Delivery Channels | Online, Mobile and Services | Organizational Characteristics | External Threats

Risk Categories (in light orange)**:** Each risk category contains a series of statements that describe risk levels. Complete each worksheet and then determine the overall inherent risk level (step 3a).

- The worksheets are:
  - Technologies and Connection Types
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Organizational Characteristics
  - External Threats
- Each worksheet has a series of questions that relate to business risk. There are two input areas:
  - **Score**: select from the options least, minimal, moderate, significant, most
  - **Notes**: an optional area to record additional, unscored information.



Note: please take care when copying from a prior year workbook. Use "paste as value" not the regular paste function.

Maturity Summary | Maturity Roll Up

Maturity Rollup and **Maturity Summary**: there are no inputs for these worksheets. They only summarize the scoring for each domain, assessment factor and component.

The heat map shading, cells `D6:H35`, in the maturity summary varies from red, at 0%, to yellow, at 50%, to green, at 100%. The calculated maturity levels are also shaded. The shading varies from red, for below baseline, to green for innovative.

Warning!

Maturity Summary

The color shading on the Maturity Summary heat map, cells `D6:H35`, only works when there are different values in the summary.

Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved

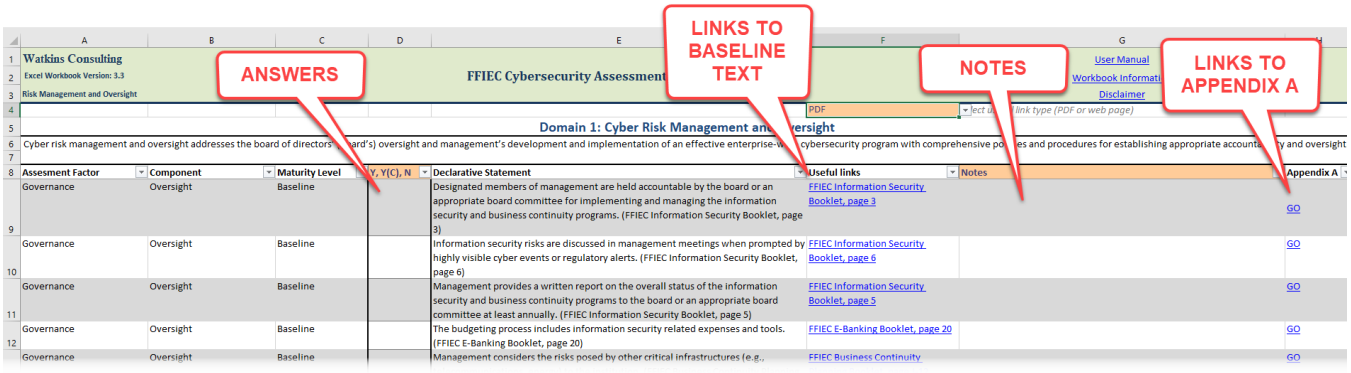
Risk Management and Oversight | Threat Intel and Collaboration | Cybersecurity Controls | External Dependency | Cyber Incidence

Domain worksheets: answer each declarative statement describing your organization risk

- Each domain has its own worksheet
  - Risk Management and Oversight
  - Threat Intel and Collaboration
  - Cybersecurity Controls
  - External Dependencies
  - Cyber Incidence
- Declarative statement organization:
  - Answer: Yes, Yes(C), No or "N/A"

If all the answers for a component's maturity level are marked as "N/A" then that level's score and all scoring for the levels above, it will be evaluated as "N/A." If you want the worksheet to score the component as passing that maturity level, at least one answer must be marked "Yes." Recommend that if you do mark an "N/A" with a "Yes" that you add a note explaining that this is to force the workbook to correctly score the component.

  - Optional information is entered in the `notes` column
  - For baseline level statements there are
    - Links to baseline text source (FFIEC booklets; links are either to the web version or the PDF version, as determined by cell `F4`).
    - Links to the Appendix A text and reference links.



Note: please take care when copying from a prior year workbook. Use "paste as value" not the regular paste function.

Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved

Pivot Reports | Table Roll Up

Two new worksheets have been added to allow you to more easily create reports. The **Table Roll Up** sheet is a table of all the maturity declarative statements. This can be used a basis for pivot table reports or charts as needed on the **Pivot Reports** worksheet. The table roll up is created by cell references and doesn't need to be refreshed; however, pivot reports should be refreshed manually after updating any declarative statements.

Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved

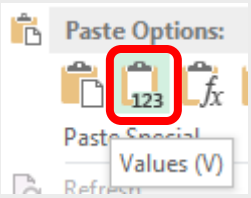
Appendix A

Appendix A contains additional reference material to understand the intent of baseline declarative statement. Each baseline cybersecurity maturity statement, has a link in column H labeled "GO." Clicking on the "GO" link will move the active workbook cell to the first informative reference for the declarative statement. Each reference has an additional link to the source document.

To return to the declarative statement, click on the "DS" link, in column D.

Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved

Troubleshooting

Problem	Solution
Link does not open in browser	• If IE is the default browser, delete browser history, close browser, open browser, try link again • Change default browser • Risk maturity worksheets may different link options (dropdown, cell `F4`) • Fix booklet URL on Information worksheet (cells `B38:B46`).
N/A maturity level score prevents risk maturity scoring from evaluating to the correct level.	Answer one of the maturity level questions "Yes" instead of "N/A." Recommend that you add a note to explain your scoring.
Problem editing text copied from other workbooks	When copying from other workbooks, use the paste as values option. Using the regular paste may result in conditional formatting and data validation errors. 
All other issues.	Contact Watkins Consulting at solutions@watkinsconsulting.com We are here to help.

Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved

Version History

Version	Date	Author	Change
1.0	10/14/2015	JMJ	Initial Version
2.0	8/11/2017	JMJ	Update for latest CAT (May 2017) and Excel workbook (version 2); added troubleshooting section
3.3	5/31/2019	JMJ	Updated formatting; added descriptions for new worksheets; new address
3.3.1	10/1/2019	JMJ	Fixed typos, grammar, added note on N/A component warning

Works Cited

[1] FFIEC, "Cybersecurity Assessment Tool (May 2017)," FFIEC, Washington, 2017.

[2] FFIEC, "FFIEC Cybersecurity Assessment Tool Overview for Chief Executive Officers and Boards of Directors," FFIEC, Washington, 2015.

[3] Watkins Consulting, Inc., "Website Privacy Policy," 2017. [Online]. Available: https://watkinsconsulting.com/privacy-policy/.

Copyright © 2019, Watkins Consulting, Inc., All Rights Reserved