FFIEC Cybersecurity Assessment Tool
Automated Scoring Using an Excel Workbook

User Guide | 2.0 | August 23, 2017

WATKINS CONSULTING

888 Bestgate Road #401
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?

CAT—a New Yes

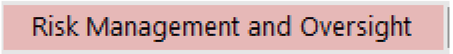
The primary change on the CAT side is that the FFIEC has added the option for the declarative statements to respond with "Yes with Compensating Controls."

Watkins Excel Workbook—Small Changes, Same Concept

We have listened to your suggestions. Beyond some formatting changes here are the changes from version 1.02.

- Firm name and report date are added to all worksheets.
- Added controlled risk indicator "Yes(C)" for risk maturity declarative statements.
- Added log worksheet.
- Broke up an unintentionally grouped declarative statements (Risk Management/Training and Culture/Culture/Evolving).

Warning!



Risk Management and Oversight

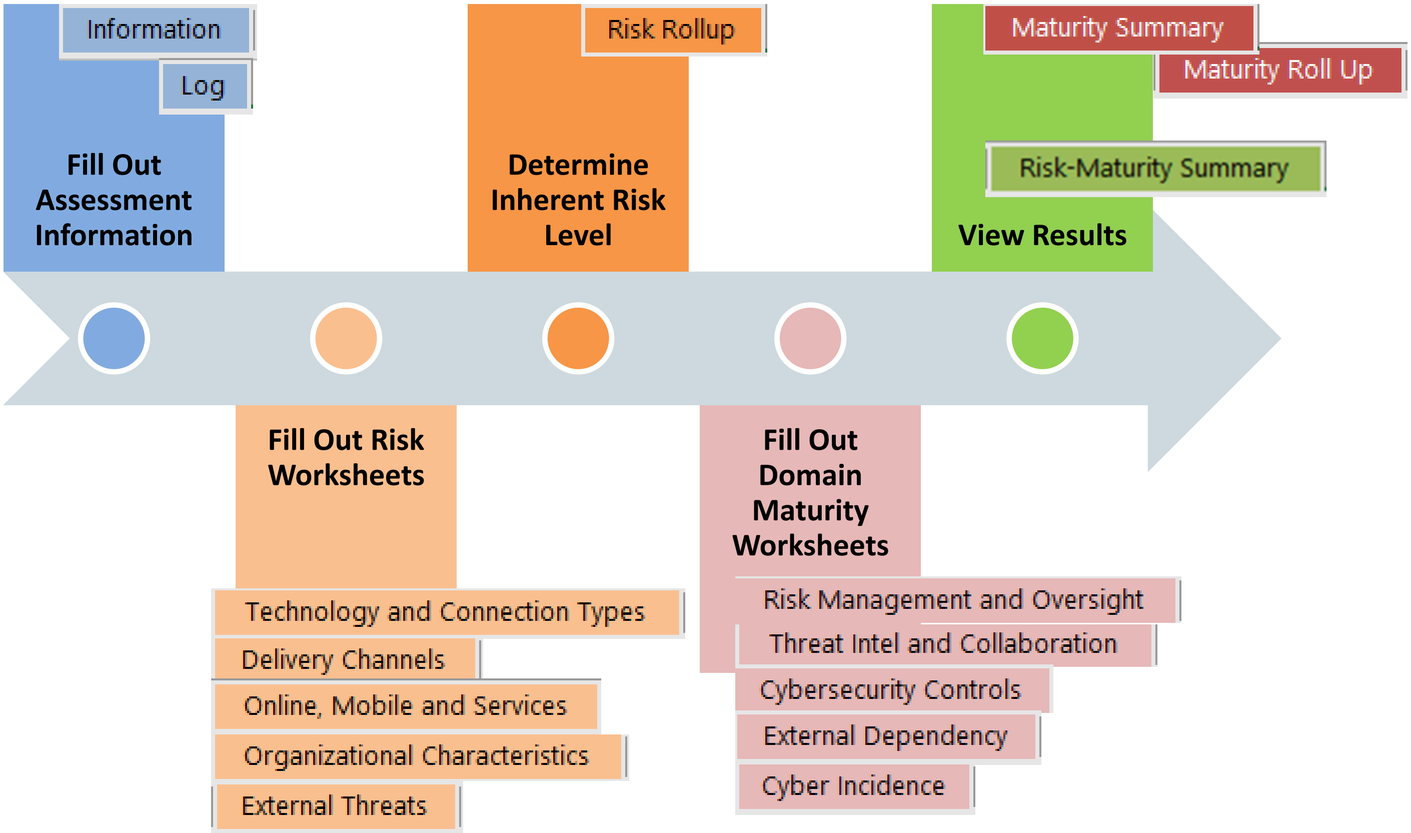
This last change is the only item which will keep you from directly cutting and pasting from your current workbook to the revised workbook. So just be careful when cutting and pasting to the **Risk Management and Oversight Risk Maturity** worksheet. Where you had one answer before, you will need to expand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

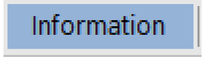
The task has been broken down into a workflow based on the CAT elements, as depicted below.

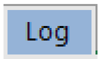

Information
Log
Fill Out Assessment Information
Risk Rollup
Determine Inherent Risk Level
Maturity Summary
Maturity Roll Up
Risk-Maturity Summary
View Results
Fill Out Risk Worksheets
Technology and Connection Types
Delivery Channels
Online, Mobile and Services
Organizational Characteristics
External Threats
Fill Out Domain Maturity Worksheets
Risk Management and Oversight
Threat Intel and Collaboration
Cybersecurity Controls
External Dependency
Cyber Incidence

Organization Details

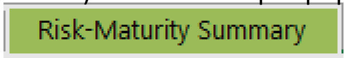
The workbook closely follows the FFIEC approach. The tool is split up into sixteen worksheets.

1. **Information**: contact, version and copyright information.
    a. 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].
    b. **Recommended Inputs**: Firm name (cell B18) and date (cell B19).
    c. **Optional Inputs**: Assessor (cell B20) and general notes (cell B21).





2. Optionally keep track of your workflow on the **Log** worksheet.
3. **Risk-Maturity Summary** (green tab): this is an output populated from the inherent risk rollup and domain maturity sections.



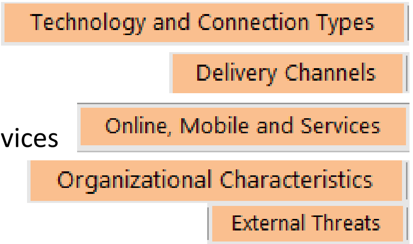
   a. The only option is in cell `I15` which allows you to select how the domains will be displayed on the matrix—by name (default) or by number.

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

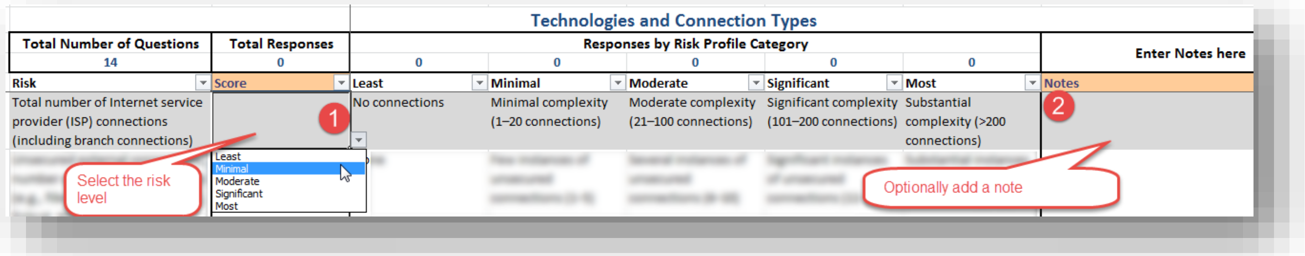
   a. **Required Input:** Overall inherent risk level (cell `C17`). Once you have completed answering the questions in the risk category worksheets, the scoring for each category will be shown above this input. Your firm should use its judgement about risk to determine the appropriate risk level (least, 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]***

5. **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).
   a. The worksheets are:
      i. Technologies and Connection Types
      ii. Delivery Channels
      iii. Online/Mobile Products and Technology Services
      iv. Organizational Characteristics
      v. External Threats


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

   b. Each worksheet has a series of questions that relate to business risk. There are two input areas:
      i. **Score**: select from the options least, minimal, moderate, significant, most
      ii. **Notes**: an optional area to record additional, unscored information.


Technologies and Connection Types

Total Number of Questions	Total Responses	Responses by Risk Profile Category					Enter Notes here
14	0	0	0	0	0	0	
Risk	Score	Least	Minimal	Moderate	Significant	Most	Notes
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)	

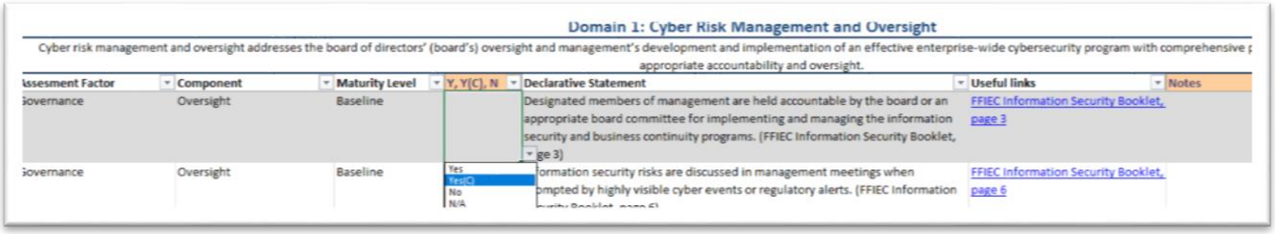
1 Select the risk level

2 Optionally add a note

6. **Maturity Rollup** and **Maturity Summary**: there are no inputs for these worksheets. They only summarize the scoring for each domain, assessment factor and component.
7. **Domain worksheets**: answer each declarative statement describing your organization risk
   a. Declarative statement organization:
      i. Answer: Yes, Yes(C), No or "N/A"

> ***Warning!** 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."*

ii. Optional information is entered in the `notes` column



Domain 1: 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 ‡ appropriate accountability and oversight.

ssesment Factor	Component	Maturity Level	Y, Y(C), N	Declarative Statement	Useful links	Notes
overnance	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. (FFIEC Information Security Booklet, ge 3)	FFIEC Information Security Booklet, page 3	
overnance	Oversight	Baseline		formation security risks are discussed in management meetings when ompted by highly visible cyber events or regulatory alerts. (FFIEC Information	FFIEC Information Security Booklet, page 6	

b. For each domain

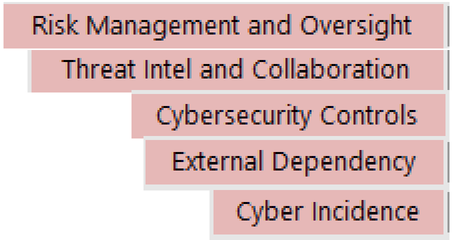
i. Risk Management and Oversight

ii. Threat Intel and Collaboration

iii. Cybersecurity Controls

iv. External Dependencies

v. Cyber Incidence



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 • Some risk maturity worksheets have 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.
All other issues.	Contact Watkins Consulting at solutions@watkinsconsulting.com We are here to help.

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

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/.