

FFIEC CYBERSECURITY ASSESSMENT TOOL AUTOMATED SCORING USING AN EXCEL WORKBOOK

User Guide | 1.0 | October 14, 2015

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* [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.

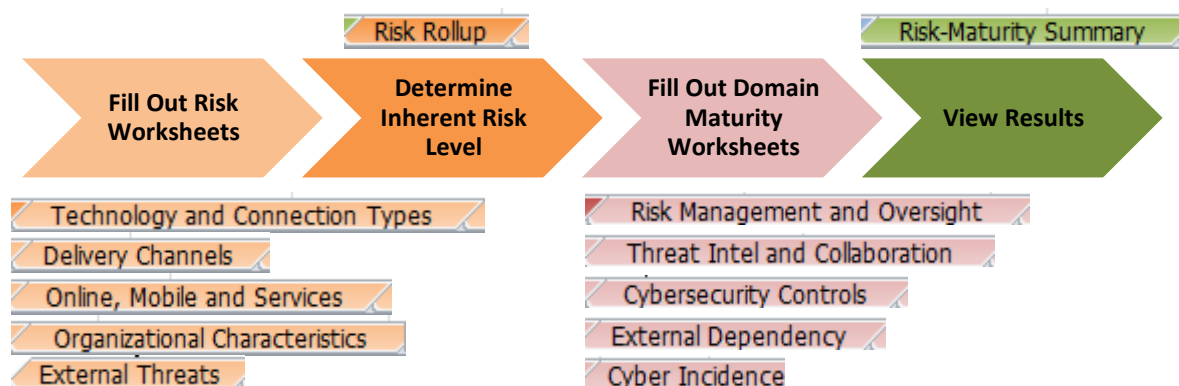
If you need help with using the tool or interpreting the results, Watkins Consulting can help with interpreting and applying the FFIEC guidelines, cybersecurity governance issues and a wide range of other cybersecurity issues, including breach remediation and penetration testing.

OBTAIN

The Excel workbook is available from the Watkins Consulting website, www.watkinsconsulting.com/FFIEC-CAT.html.

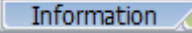
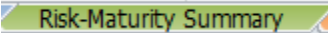
THE PROCESS

Answer the cybersecurity assessment questions to determine your business' risk-maturity. The questions are distributed on the risk, the risk rollup, and the domain maturity worksheets. The scoring is summarized on the risk-maturity summary worksheet.



ORGANIZATION DETAILS

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

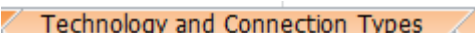
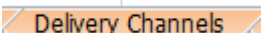
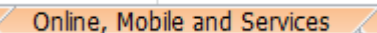
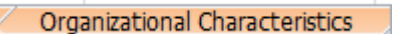
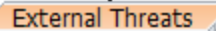
1. **Information** : contact, version and copyright information. 
 - a. We recommend that you use the link in cell A8 to send us your email so that we can notify you of updates. We will not share your information, per our on-line privacy policy [3].
2. **Risk-Maturity Summary** (green tab): this is an output populated from the inherent risk rollup and domain maturity sections. 
 - a. The only option is in cell I16 which allows you to select how the domains will be displayed on the matrix—by name (default) or by number.
3. **Risk Rollup** (orange tab): this summarizes the inherent risks associated with each risk category.

Risk Rollup

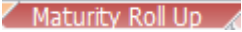
- a. **Required Input:** Overall inherent risk level (cell C24). Once you have completed answering the questions in the risk category worksheets, the scoring for each category will be shown above this input. Your firm will have to use its judgement about risk to determine the appropriate risk level (least, 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]

- b. **Optional Inputs:** Firm name (cell C9), assessor (cell C10), date (cell C11).
4. **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 
 - 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.

Total Number of Questions		Total Responses		Technologies and Connection Types					Enter Notes here
14		0		Responses by Risk Profile Category					
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)			
							Optionally add a note		

5. **Maturity Rollup:** there are no inputs in this spreadsheet. It only summarizes the scoring for each domain, assessment factor and component. 
6. **Domain worksheets:** answer each declarative statement describing your organization risk
 - a. Declarative statement organization:
 - i. Answer: Yes, No or "N/A"

Warning! *If all of 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."*

Domain 3: Cybersecurity Controls						
Assessment Factor	Component	Maturity Level	Y,N	Declarative Statement	Useful links	Notes
Preventative Controls	Infrastructure Management	Baseline		Network perimeter defense tools (e.g., border router and firewall) are used. (FFIEC Information Security Booklet, page 33)	Information Security Booklet (PDF)	

Answer each question

Add optional information

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

b. For each domain

- i. Risk Management and Oversight 
- ii. Threat Intel and Collaboration 
- iii. Cybersecurity Controls 
- iv. External Dependencies 
- v. Cyber Incidence 

VERSION HISTORY

Version	Date	Author	Change
1.0	10/14/2015	JMJ	Initial Version

WORKS CITED

- [1] FFIEC, "Cybersecurity Assessment Tool," FFIEC, Washington, 2015.
- [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," Watkins Consulting, Inc., Annapolis, 2015.