NIST Cybersecurity Framework (1.0)
Tracking Evaluations Using an Excel Workbook

User Guide | 2.0 | January 8, 2018

WATKINS CONSULTING

888 Bestgate Road #401
Annapolis, MD 21401
solutions@watkinsconsulting.com

www.watkinsconsulting.com

Summary

This is a companion user guide for the Excel workbook created by Watkins Consulting to automate tracking and scoring of evaluation activities related to the NIST Cybersecurity Framework (CSF) [1] with NIST 800-53 rev 4 [2] controls and FFIEC Cybersecurity Assessment Tool mapping [3]. This user guide assumes that NIST CSF documentation is used to determine your firm's appropriate cybersecurity risk management approach. This user guide only describes how to use the Watkins Consulting Excel workbook ('Workbook').

If you need help with using the Workbook or interpreting the results, Watkins Consulting can help your firm with the Workbook and more: cybersecurity governance issues and assessments.

Obtain

The Workbook is available from the Watkins Consulting website, http://www.watkinsconsulting.com/NIST-CSF.html. This user guide is the companion for workbook version 2.2.

Register

We recommend that you send us an email using the registration link (*Information* worksheet, `cells A7:B8`). We will not share your information outside of our organization and after confirming your registration, we will notify you of any updates or potentially helpful information related to the Workbook.

Organization

The Workbook has five visible worksheets.

- **Information**: describes the workbook and has some formatting controls.
- **Rollup**: summarizes the status value by category.
- **CSF Core**: Contains the functions, categories, sub-categories, and informative references [1].
- **800-53 Controls:** 800-53 rev 4 controls downloaded from NIST [2] and designed to provide an interactive reference for the CSF informative references.
- **FFIEC CAT Core Map:** automatically maps the *CSF Core* responses to the FFIEC CAT June 2015 mapping [3].

There is also one hidden worksheet, *References*, which contains tables used to make the workbook flexible and responsive (user input validation lists, etc.).

HOW TO USE THE WORKBOOK

Start with the CSF Core tab

To facilitate your record keeping, there are four input fields at the top of the *CSF Core* worksheet.

- Assessment date, will be shown on *Rollup* worksheet.
- Firm name, will be shown on *Rollup* worksheet.
- Responsible Party
- General Notes

Although there is no standardized way to evaluate your firm's approach to applying the framework to your cybersecurity strategy, this workbook uses an implied approach. It is designed to review each of the 98 sub-categories found on the *CSF Core* worksheet. For each sub-category, you can input the status of your firm's cybersecurity practice, perhaps as informed by the informative references for each sub-category. This workbook allows for one of four "`Status`" values.

- Yes
- No
- N/A
- Blank

As you begin, all the response values are set to "`blank`." This will indicate that the sub-category has not been reviewed. For sub-categories that do not apply to your firm answer "N/A." If, in your evaluation, your firm has adequate risk controls in place or accepts the level of risk for the sub-category then answer "`Yes`". If not then answer "No." Figure 1 depicts a screen capture of the worksheet for the ID.AM-1 sub-category.

In addition to setting the "`Status`" field (`column D`), specific details may be added to the "`Notes`" field (`column G`).

Warning! ***Do not use the paste functionality to fill in the "`Status`" value; it could work in an unpredictable manner.***

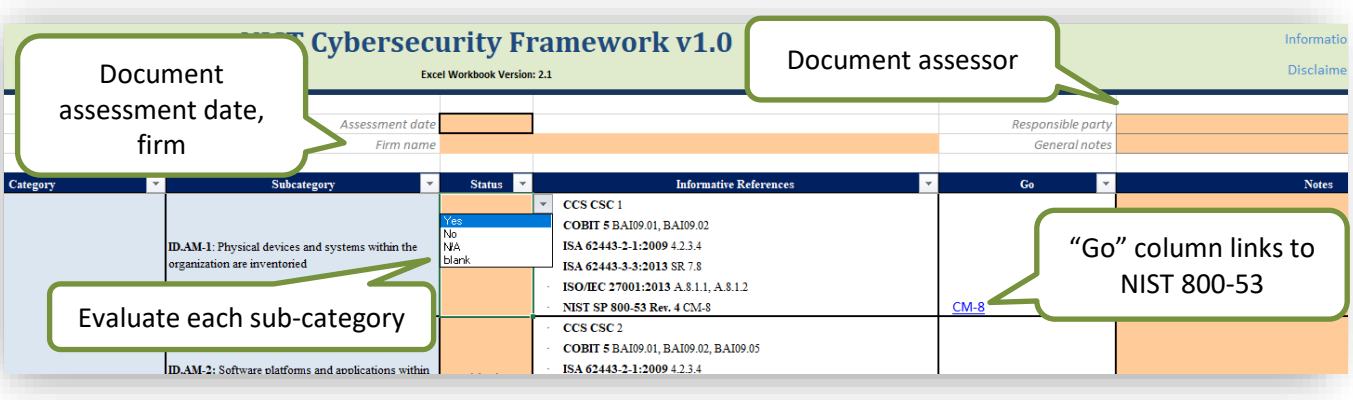

Figure 1 A partial view of the *CSF Core* worksheet. The first sub-category in the Identify (ID) function's Asset Management (AM) category is shown. The drop-down for the "`Status`" field shows the allowed answers: `yes`, `no`, `N/A`, and `blank`. A note may be added for each sub-category. It is also recommended that the assessment date, assessor and firm name for the overall evaluation be recorded.

The "Go" Column: Hyperlinks to the Risk Controls

When assessing each sub-category, if the NIST 800-53 rev 4 controls are of interest, it is possible to use the "Go" column hyperlink to view the controls for the sub-category. Click on the hyperlink to display the *800-53 Controls* worksheet, the controls list will be filtered to display the appropriate control(s).

Excel hint: since the informative references use intra-workbook hyperlinks, it is convenient to add the Back and Forward Excel commands to the quick access toolbar.

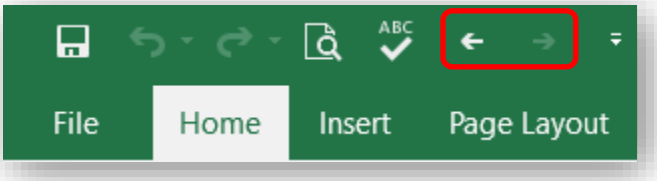

Figure 2 The Excel quick access menu with the "Back" and "Forward" commands added.

Reset All Responses to Blank

Since it is inconvenient to copy and paste or even select the merged cells used in the `Status` column, functionality to reset all the responses to the blank state is provided by a button, located near `cell B6`, labelled "RESET FORM." To reset all the status input cells to "blank" values, click the RESET FORM button and then click the `Yes button` in response to the "Are you sure" question.

The Rollup Summary

The *Rollup* worksheet summarizes the sub-category status responses by category and function, providing a summary of which sub-categories have been evaluated. The Rollup is only intended to help measure the scoring with respect to the "`Yes`" values. It displays a percentage of the status values that have been set to "`Yes`" without including the not-applicable sub-categories. The formula used is:

$$\text{Score} = N_{yes} \;/\; (N_{yes} + N_{no} + N_{blank}) \qquad [1]$$

This is equivalent to:

$$\text{Score} = N_{yes} \;/\; (N_{total} - N_{N/A}) \qquad [2]$$

There are three possible scoring results.

- A percentage from 0% to 100%
- A single dash, "-", which indicates that too few sub-categories have been assigned from the "blank" initial state (controlled by the minimum number of question level set in the *Information* worksheet)
- A double dash, "--", which indicates an error condition in the calculation

Warning—this score may have little relationship to the actual risk that your firm is exposed to in each category. But it can provide a helpful visual snapshot of the evaluation, especially when compared to evaluations made at various times.

Reference Material Worksheets

800-53 Controls

This worksheet can be used independently of the hyperlinks from the *CSF Core* worksheet. It is a reformatted version of the NIST material with an extra field, "Control" in `column B`, that can be used with the Excel filter function. Or, the filter control input, `cell B11`, can be used to set the filter inputs by entering the desired controls in a comma delimited list (for example, "AC-1, AU-3" without the quotes).

Cybersecurity Assessment Tool Mapping

There is no user-interactive functionality in this worksheet. It simply reports the CSF sub-category assessed value in `column E` as defined by the mapping of the sub-category, `column D`, to the FFIEC CAT declarative statement, `column F`.

TECHNICAL CONSIDERATIONS

Warning—Don't Use Paste Functionality for The Status Field

Each of the 98 status cells must be individually updated. The normal Excel copy or cut and paste functionality may not work as anticipated because of the underlying merged cell construction.

Controls—Format the Shading

There are three controls that affect how the scoring is displayed. They are in the *Information* worksheet in cells `A36:A38`. The controls and their default values are as follows.

1	*Minimum number of questions to answer for roll up score to be calculated*
33%	*All category rollup scores below this value are shaded in red*
66%	*All category rollup scores above this value are shaded in green*

Answers falling between the green and red scores are shaded in yellow. If you want to turn off the conditional shading, set the minimum number to at least 13, which is one more than the maximum number of sub-categories found in any category.

The red, yellow, and green shading is arbitrary and should be adjusted to fit your firm's level of risk acceptance.

Assessment Date Limits

To improve the quality control of user inputs, an acceptable date range for the assessment date may be specified in the controls. The default is a very wide range.

1/1/2010	*first allowed assessment date*
12/31/2030	*last allowed assessment date*

The assessment date is also verified to be a date input.

Protection—only the input cells should be changed

The Workbook is password protected to maintain formula integrity and textual information. Only cells displayed as input cells (orange background, dark purple text, grey border) are unlocked. If your firm needs a special version of the workbook or has suggestions for improvements, we are open to making those updates.

Macros

Previous versions of the Workbook were macro free; however, to provide the reference linkage for the NIST 800-53 two subroutines were added. Both macros are triggered by changes to the worksheets that they are associated with. The first is `Worksheet_SelectionChange` and is in the *CSF Core* and the second is `Worksheet_Change` in *800-53 Controls*.

A pair of macros was also added to the *CSF Core* worksheet to enable the clear all answers functionality. These are `Reset_Form`, which asks the user if they really want to clear all the non-blank answers, and `Blank_All`, which sets all the answers to blank.

A macro-free workbook is available upon request.

VERSION HISTORY

User Guide Version	Excel Workbook Version	Date	Author	Change
1.0	1.02	4/18/2017	JMJ	Initial Version
2.0	2.2	1/16/2017	JMJ	Updates to match 2.2: added in 800-53 and FFIEC CAT, VBA macros

WORKS CITED

[1] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," NIST, Gaithersberg, MD, 2014.

[2] NIST, "NIST Special Publication 800-53 Revision 4," NIST, Gaithersburg, 2015.

[3] Federal Financial Institutions Examination Council, "FFIEC Cybersecurity Assessment Tool," Federal Financial Institutions Examination Council, Washington, 2017.

