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

User Guide | 3.11 | February 21, 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 and NIST 800-53 documentation is used to determine your firm's appropriate cybersecurity risk management approach. Some additional Excel columns have been made available to the user to add some risk management information.

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 3.1.

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

Macros have been added to the Excel workbook to help with the 800-53 controls look-up and to allow the two status methods to co-exist. Depending on your Excel settings you may be prompted with a security warning to Enable Content. Please allow macros to be enabled.

Start with the CSF Core tab

To facilitate your record keeping, there are four input fields at the top of the *CSF Core* worksheet. These are shown in Figure 1.

- 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 two methods to describe the sub-category status: binary (yes or no) and senary (0-5). The binary method is the default. If you want to switch to the senary method, please do so before changing the `Status` column cells (or you can reset the fields to blank after changing methods). To switch between the two methods, select the desired method on the *Information* worksheet in the controls region, cell `A41`. If you do change the method, please change the shading cutoff values for the Rollup worksheet in cells `A37:A38` (typically .33 and .66 for the binary method and 2 and 4 for the senary method).

Binary: Yes/No	Senary: 0–5
• **Yes** • **No** • **N/A** • **Blank**	• 0 • 1 • 2 • 3 • 4 • 5 • 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`." For the binary methods when 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." Likewise for the senary method, use your risk evaluation to scale the risk control as an integer from 0 to 5. Figure 1 depicts a screen capture of the worksheet for the ID.AM-1 sub-category.

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

Warning! ***Please use the paste-as-value functionality if you are pasting "`Status`" values; otherwise, the worksheet could work in an unpredictable manner due to validation errors.***

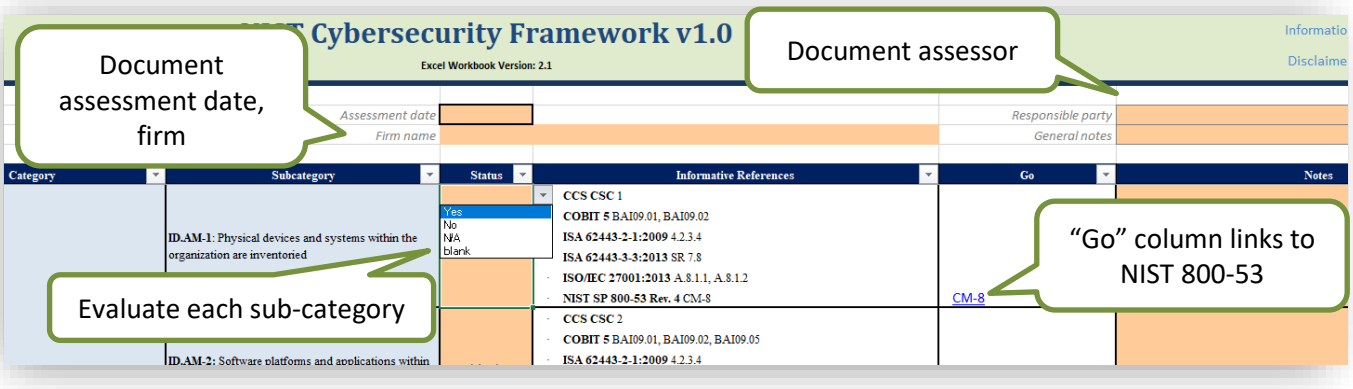

Figure 1 A partial view of the *CSF Core* worksheet. The first sub-category in the Identify (ID) function's Asset Management (AM) category is shown. The drop-down for the `Status` cell shows the allowed answers: `yes`, `no`, `N/A`, and `blank` for the binary input method. A note may be added for each 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 Status Field Responses to Blank

Functionality to reset all the responses to the blank state is provided by a button, located near `cell B6`, labelled `Set All Status Column Answers to "Blank"`. To reset all the status input cells to "blank" values, click the reset button and then click the `Yes button` in response to the "Are you sure" question.

Risk Management

To the right, `columns H:AI`, of this basic tracking functionality 28 columns/fields have been added to help facilitate risk management actions taken for each sub-category. These are summarized in the table below.

These optional fields are designed to track your risk management strategy, the baseline risk, the effect of current controls, the current risk, the goal and the gap between the current state and the goal. To aid in prioritization of resource allocation, estimated losses associated can be calculated for the baseline and current state. Also, to help relate the current effectiveness of the controls, the user can enter a formula in the `Status Calculation` column to calculate a "Status" value. This can then be copied and **pasted-as-value** into the `Status` column (use of this is optional and it does require Excel expertise). A sample formula has been included.

Field	Function	Purpose
Confidentiality Impact (baseline)	User Input	Evaluation of confidentiality impact: Low, Medium, High.
Integrity Impact (baseline)	User Input	Evaluation of Integrity impact: Low, Medium, High.
Availability Impact (baseline)	User Input	Evaluation of Availability impact: Low, Medium, High.
Security Category (Risk Impact baseline)	Calculation	Maximum of CIA impacts.
Risk Likelihood (baseline)	User Input	Evaluation of risk likelihood: Low, Medium, High.
Risk (baseline)	Calculation	Security Category (Risk Impact) and Likelihood values are mapped to a numerical score based on information worksheet control `cells A44:A45` and then multiplied. For instance, a "Low impact" and a "High likelihood" for a scaled 1-3 basis would be evaluated as a 3=1*3. [2, p. 28]
Risk Strategy	User Input	Preferred strategies are limited to: avoid, accept, mitigate, transfer, and other.
Control Description	User Input	Describe your control(s).
Compensating Control Description	User Input	If the controls associated with this risk are supplemented by other controls, describe those controls here.
Controlled Confidentiality Impact (current state)	User Input	Evaluation of confidentiality impact with controls in place: Low, Medium, High.
Controlled Integrity Impact (current state)	User Input	Evaluation of integrity impact with controls in place: Low, Medium, High.
Controlled Availability Impact (current state)	User Input	Evaluation of availability impact with controls in place: Low, Medium, High.
Controlled Impact (current state)	Calculation	Maximum of controlled CIA impacts.
Controlled Likelihood (current state)	User Input	Evaluation of controlled risk likelihood: Low, Medium, High.
Controlled Risk (current state)	Calculation	Same as risk calculation, but using controlled risk impact and controlled likelihood.
Risk Reduction Controlled Risk – Risk (current state – baseline)	Calculation	Controlled risk minus the uncontrolled risk (negative is better).
Risk Goal	User Input	Risk goal for this sub-category.

Field	Function	Purpose
Risk Gap	Calculation	Controlled risk – risk goal (smaller is better). Will display "--" for a blank risk goal.
Potential Loss at Maximum Risk	User Input	Evaluation of the maximum loss associated with this sub-category **when risk impact and likelihood are both High**. Set to 100 to simulate percentage, but should reflect importance to firm relative to other sub-categories. Note, `cell Z8` shows the maximum risk, which is the High scale mapping value squared.
Uncontrolled Loss (baseline)	Calculation	Potential loss at maximum risk multiplied by the fraction of (risk-risk minimum)/risk range. This fraction should scale the risk as to 0% at the minimum value to 100% at the maximum value. Example, if risk is Low and likelihood is High when the mapping values are 1 for Low and 3 for High, the Risk is 3=1*3, which is 33% of the maximum risk scale, 9=3*3. So, for a maximum potential loss of 100, the uncontrolled loss would be 33.
Controlled Loss (current state)	Calculation	The same calculation method as for uncontrolled loss, but using controlled loss as the input to the fraction.
Loss Benefit	Calculation	The percentage of the change in loss as calculated from (Uncontrolled Loss – Controlled Loss)/Uncontrolled Loss. 100% is the best. Errors result will be shown as a hyphen.
Control Implementation Date	User Input	Help to identify the control by entering the date here.
Status Calculation	User Input	Enter you Excel formulas here to calculate what you need.
Risk Owner	User Input	Risk owner's name.
Audit Reference	User Input	If applicable, the audit used to determine the risk control(s)' effectiveness.
Assessment Reference	User Input	If applicable, the assessment used to determine the risk control(s)' effectiveness.
Risk Management Status	User Input	Any additional information about the risk management progress.

Table 1 Risk Management Fields

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 binary or senary values. The binary method is scored from 0%-100% while the senary method is scored from 0-5. For both calculations a single dash, "-", 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, cell `A36`) while a double dash, "--", which indicates an error condition in the calculation.

Binary Method: Yes/No	Senary Method: 0-5
Displays a percentage of the status values that have been set to "`Yes`" without including the not-applicable sub-categories. The formula used is: $\text{Score} = \frac{Nyes}{Nyes + Nno + Nblank}$ [1] This is equivalent to: $\text{Score} = \frac{Nyes}{Ntotal - Nn/a}$ [2]	Average of all the values that are not marked as N/A, with "blank" values evaluated as zeros. Should result in a value from 0-5. $\text{Score} = \frac{N_1 + 2{*}N_2 + 3{*}N_3 + 4{*}N_4 + 5{*}N_5}{N_0 + N_1 + N_2 + N_3 + N_4 + N_5 + Nblank}$ [3]

Optionally, the scoring may leave out the unanswered, "blank" questions; this is controlled with `cell A46` in the controls section on the *Information* worksheet.

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 status of your evaluation progress.

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—Use Paste-As-Value Functionality for The Status Field

The normal Excel copy or cut and paste functionality may not work as anticipated because of the underlying data validation. Use the paste-as-value option.

Controls—Format the Shading

There are three controls that affect how the scoring is displayed. They are in the *Information* worksheet in cells A36:A45. The controls and their default values are as follows.

1	*Minimum number of questions to answer for roll up score to be calculated*
0.33	*All category rollup scores below this value are shaded in red*
0.66	*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. These are related to the scoring method selected, and should be changed when the scoring method is changed.

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.

Scoring Method

Select the desired scoring method

yesNoNA	*select the scale for answers (should also select desired rollup shading values above)*

Output Controls

The values shown for calculation errors and where inputs have not been defined may be updated here.

-	*Calculation Error Output*
--	*Calculation None Output*

Risk Scaling

Set the low and high numeric equivalents for risk and likelihood numeric calculations.

1	*Low Numeric Score (must be >0)*
3	*High Numeric Score (must be greater than low score)*

Counting Blanks in the Scoring

This Yes/No option controls if "blank" values are included in the averages as a No or zero.

Yes	*Include "blank" count in score calculation*

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
3.1	3.1	2/21/2018	JMJ	Updated for risk management section.
3.11	3.1	3/15/2018	JMJ	Clarified paste-as-value and columns/fields language

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.

