Table of Contents

[Overview 3](#_Toc429746275)

[Structure 3](#_Toc429746276)

[Named Groups 3](#_Toc429746277)

[Common Functions 4](#_Toc429746278)

[INDIRECT 4](#_Toc429746279)

[Example 4](#_Toc429746280)

[AppDesc 4](#_Toc429746281)

[Maintenance 5](#_Toc429746282)

[DocumentationRisk 5](#_Toc429746283)

[Maintenance 5](#_Toc429746284)

[NeverEvents 5](#_Toc429746285)

[Maintenance 5](#_Toc429746286)

[NoBackupInfo 6](#_Toc429746287)

[Maintenance 6](#_Toc429746288)

[NoDataClass 6](#_Toc429746289)

[Maintenance 6](#_Toc429746290)

[NoOwner 6](#_Toc429746291)

[Maintenance 6](#_Toc429746292)

[RiskDetails 6](#_Toc429746293)

[RiskScore 7](#_Toc429746294)

[Maintenance 7](#_Toc429746295)

[RiskTrend 7](#_Toc429746296)

[Maintenance 7](#_Toc429746297)

[TechnicalRisk 7](#_Toc429746298)

[Maintenance 8](#_Toc429746299)

[TrendTeam 8](#_Toc429746300)

[Maintenance 8](#_Toc429746301)

[TypeOfRisk 8](#_Toc429746302)

[Maintenance 8](#_Toc429746303)

[UnsupportedOSRisk 8](#_Toc429746304)

[Maintenance 9](#_Toc429746305)

[Scorecard 9](#_Toc429746306)

[Structure 9](#_Toc429746307)

[Application Name 9](#_Toc429746308)

[Formulas or Conditional Formatting 10](#_Toc429746309)

[Risk Score 10](#_Toc429746310)

[Formulas or Conditional Formatting 10](#_Toc429746311)

[Type of Risk 10](#_Toc429746312)

[Formulas or Conditional Formatting 10](#_Toc429746313)

[NeverEvents 10](#_Toc429746314)

[Formulas or Conditional Formatting 10](#_Toc429746315)

[Trend 11](#_Toc429746316)

[Formulas or Conditional Formatting 11](#_Toc429746317)

[Description 11](#_Toc429746318)

[Formulas or Conditional Formatting 11](#_Toc429746319)

[Date 11](#_Toc429746320)

[Apps 11](#_Toc429746321)

[Formulas or Conditional Formatting 11](#_Toc429746322)

[Scoring 11](#_Toc429746323)

Information Security Risk Scorecard - Applications

# Overview

The *Information Security Risk Scorecard - Applications* (“Risk Scorecard”) is intended to normalize and measure common areas of risk for applications. The goal is not to measure every area of risk, but to highlight things that are of significant risk or which serve as a leading indicator of a larger problem.

For each area of risk a value has been assigned, the goal is to get a lower score, so the areas I want people to focus on first have a higher value.

# Structure

There are 6 tabs within the Risk Scorecard:

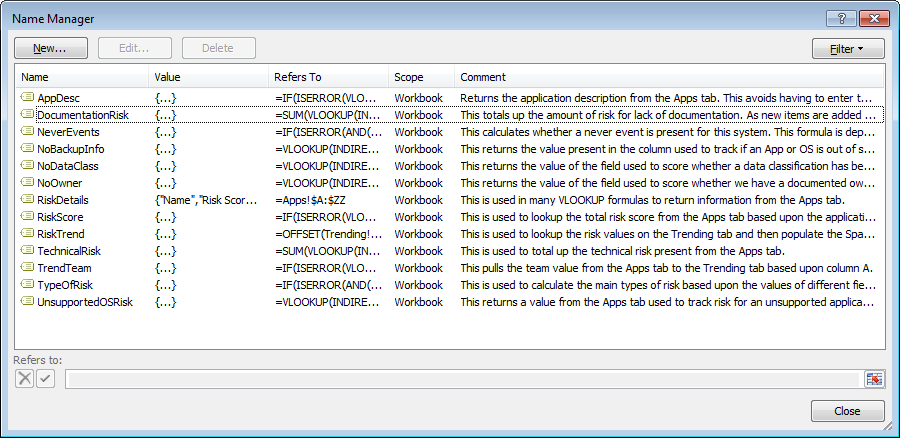
1. Scorecard
2. Apps
3. Scoring
4. Trending
5. Chart Data
6. Version Notes

Each tab in the Risk Scorecard will be covered below. In addition there are 13 named groups which are used in formulas on the various tabs. The use of named groups will allow the scorecard to dynamically update with few changes and are critical to understanding how the scorecard functions.

## Named Groups

Named groups are aliases to a range of cells or a formula; they are critical to this file. This makes formulas cleaner and allows the use of some formulas, such as INDIRECT, in places where it would not normally work.

Each named group will be detailed, covering the intent of the named group, the formula used and explaining why the formula was structured that way along with any expected maintenance.



Formulas > Defined Names > Name Manager in Excel

### Common Functions

There are only a few functions used in the named groups and they are in recurring patterns. The named groups primarily use ISERROR, VLOOKUP and INDIRECT. Only INDIRECT is covered below because it is not a common formula many people use in Excel.

#### INDIRECT

The INDIRECT function allows a formula to use dynamic references based upon the cell it is calculated in. If a new column is added on the Scorecard tab, any cell shifted to the right that contains a formula using the INDIRECT function will need to be updated with the new index. Most formulas in this document use INDIRECT to find the application name as part of the VLOOKUP formula.

##### Example

In the example **INDIRECT("RC[-1]",0)**, the current cell will have the value of the cell one to the left; R[1]C would get the value one row above the current cell and R[-1]C[1] would get the value one row below and one cell to the right of the current cell.

### AppDesc

The AppDesc named group is used to look up the application description. Because an application can appear multiple times on the Scorecard tab we want to make sure the description in column G is consistent. The formula used is:

**=IF(ISERROR(VLOOKUP(INDIRECT("RC[-6]",0),RiskDetails,3,FALSE))," ",IF(VLOOKUP(INDIRECT("RC[-6]",0),RiskDetails,3,FALSE)=0," ",VLOOKUP(INDIRECT("RC[-6]",0),RiskDetails,3,FALSE)))**

This formula performs a VLOOKUP on the RiskDetails named group using INDIRECT to get the value in column A for the key; it returns the third column in the RiskDetails named group, or column C of the Apps tab. ISERROR is used to ensure a blank value in column A of the Scorecard tab does not produce #N/A errors.

#### Maintenance

There is no maintenance to be performed unless a new column is inserted before C on the Apps tab.

### DocumentationRisk

This named group totals up the numeric value for any column on the Apps tab that is considered a documentation risk. The specific formula is:

**=SUM(VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,5,FALSE),VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,7,FALSE),VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,8,FALSE),VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,9,FALSE),VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,10,FALSE),VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,13,FALSE),VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,14,FALSE),VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,18,FALSE))**

This named group is used in other formulas to avoid retyping this list of VLOOKUP and INDIRECT formulas.

#### Maintenance

If new things to measure are added on the Apps tab this named group will need to be updated to ensure the column references are still accurate. If new measurements are added which would be considered documentation they will need to be added into this named group.

### NeverEvents

This named group was built to look for things that should never be present. In our cast that is currently the lack of documented backups, no defined data classification and no documented owner. The formula used is below:

**=IF(ISERROR(AND(NoBackupInfo=0,NoDataClass=0,NoOwner=0)), " ",IF(AND(NoBackupInfo>0, NoDataClass>0, NoOwner>0),"No Backup Info, Data Classification or Owner",IF(AND(NoBackupInfo>0, NoDataClass>0, NoOwner=0),"No Backup Info or Data Classification", IF(AND(NoBackupInfo>0, NoDataClass=0, NoOwner=0),"No Backup Info", IF(AND(NoBackupInfo=0, NoDataClass>0, NoOwner>0),"No Data Classification or Owner", IF(AND(NoBackupInfo=0, NoDataClass=0,NoOwner>0),"No Owner", IF(AND(NoBackupInfo=0, NoDataClass>0, NoOwner=0),"No Data Classification", IF(AND(NoBackupInfo>0, NoDataClass=0, NoOwner>0),"No Backup Info or Owner", "None"))))))))**

This formula references three named groups to make maintenance easier.

#### Maintenance

There is no maintenance with this named group unless you want to change what is considered a never event.

### NoBackupInfo

This named group performs a VLOOKUP on one cell in the Apps tab based upon the value in column A of the Scorecard tab for the selected row. The formula is:

**=VLOOKUP(INDIRECT("RC[-4]",0),RiskDetails,5,FALSE)**

The purpose of this named group is to make it easier to update the NeverEvents named group, which references this named group, if the structure of the Apps tab changes.

#### Maintenance

If you move columns on the Apps tab this named group may need to be updated.

### NoDataClass

This named group performs a VLOOKUP on one cell in the Apps tab based upon the value in column A of the Scorecard tab for the selected row. The formula is:

**=VLOOKUP(INDIRECT("RC[-4]",0),RiskDetails,7,FALSE)**

The purpose of this named group is to make it easier to update the NeverEvents named group, which references this named group, if the structure of the Apps tab changes

#### Maintenance

If you move columns on the Apps tab this named group may need to be updated.

### NoOwner

This named group performs a VLOOKUP on one cell in the Apps tab based upon the value in column A of the Scorecard tab for the selected row. The formula is:

**=VLOOKUP(INDIRECT("RC[-4]",0),RiskDetails,10,FALSE)**

The purpose of this named group is to make it easier to update the NeverEvents named group, which references this named group, if the structure of the Apps tab changes

#### Maintenance

If you move columns on the Apps tab this named group may need to be updated.

### RiskDetails

The RiskDetails named group is used when performing VLOOKUPs against the risk data on the Apps worksheet. Specifically the entry is:

**=Apps!$A:$ZZ**

Because column references are used this named reference will never need to be changed unless you want to include additional data in the VLOOKUP queries or you change the structure of the Apps worksheet. The named group goes to ZZ to ensure that future columns are part of the group, if you add columns past ZZ this formula will need to be updated.

### RiskScore

The RiskScore named group is used to populate the risk score value on the Scorecard worksheet in column B from the Apps worksheet. The key used for this lookup is the application name in column A on each sheet. The formula used is:

**=IF(ISERROR(VLOOKUP(INDIRECT("RC[-1]",0),RiskDetails,2,FALSE))," ",VLOOKUP(INDIRECT("RC[-1]",0),RiskDetails,2,FALSE))**

This formula performs a VLOOKUP query looking for a value within the named group RiskDetails, which in turn uses the INDIRECT function to retrieve a key for this lookup. INDIRECT is looking at the value one column to the left of where this named group is used (**INDIRECT("RC[-1]",0)**).

Once the correct row is found the value in the second column of the named group is returned, which will be the total risk score. By using ISERROR we can return a blank value if any error is generated, such as a typo in the name resulting in no value returned, a blank value in the range returned through the RiskDetails named group or a #N/A if a value needed in the formula is blank. The #N/A error happens most often when this is used in a blank row, since there is no value in column A to search on.

#### Maintenance

This formula does not need to be updated unless the Scorecard or Apps worksheet structure change.

### RiskTrend

For the Sparkline used on the Scorecard tab in column F to properly display the desired information, we need to determine what to search on within the Scorecard tab, where that value appears in the Trending tab and then specify what values to return from the Trending tab. This is done with a combination of the OFFSET, MATCH and INDIRECT formulas. The formula used is:

**=OFFSET(Trending!$A$1,MATCH(INDIRECT("RC[-3]",0),Trending!$A:$A,0)-1,2,1,4)**

#### Maintenance

Every time a new scorecard is released this named group will need to be updated to increase the highlighted value. However updating this one formula will update every Sparkline. The highlighted value 4 says to return four cells of data in one row from the matched value on the Trending tab (**Trending!$A:$A**) using the value three cells to the left of the current cell (**INDIRECT("RC[-3]",0)**). When the next version of scorecard is released the highlighted number should be increased to 5 so that the new data is included in the Sparkline display used on the Scorecard tab.

### TechnicalRisk

This named group totals up the numeric values associated with technical risk. This is used in the TypeOfRisk named group. The formula used is:

**=SUM(VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,20,FALSE),VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,21,FALSE))**

#### Maintenance

This named group will only need to be updated if new columns are added on the Apps tab before T.

### TrendTeam

This named group looks up the team value from the Apps tab based upon the system name in column A of the Trending tab.

**=IF(ISERROR(VLOOKUP(INDIRECT("RC[-1]",0),RiskDetails,4,FALSE))," ",VLOOKUP(INDIRECT("RC[-1]",0),RiskDetails,4,FALSE))**

#### Maintenance

There is no maintenance unless columns are added before D on the Apps tab.

### TypeOfRisk

This named group looks at the value of DocumentationRisk, TechnicalRisk and UnsupportedOSRisk to determine if any are over 5,000 points. Any of them over 5,000 points are called out in column B of the Scorecard tab. The formula used is:

**=IF(ISERROR(AND(DocumentationRisk=0,TechnicalRisk=0,UnsupportedOSRisk=0))," ",IF(AND(DocumentationRisk>4999,TechnicalRisk>4999,UnsupportedOSRisk>0),"Documentation, Technical and Unsupported OS",IF(AND(DocumentationRisk>4999, TechnicalRisk>4999,UnsupportedOSRisk=0),"Documentation and Technical",IF(AND(DocumentationRisk<4999,TechnicalRisk>4999,UnsupportedOSRisk>0),"Technical and Unsupported OS",IF(AND(DocumentationRisk>4999,TechnicalRisk<4999,UnsupportedOSRisk>0),"Documentation and Unsupported OS",IF(AND(DocumentationRisk>4999,TechnicalRisk<4999,UnsupportedOSRisk=0),"Documentation",IF(AND(DocumentationRisk<4999,TechnicalRisk>4999,UnsupportedOSRisk=0),"Technical",IF(AND(DocumentationRisk<4999,TechnicalRisk<4999,UnsupportedOSRisk>0),"Unsupported OS", "No major risks identified." ))))))))**

Named groups are used in this formula for legibility, maintenance and to keep the length short enough for Excel. If you use VLOOKUPs in place of the named groups that are part of this formula it will be too long for use in a named group.

#### Maintenance

The maintenance for this named group would be done through the referenced name groups: DocumentationRisk, TechnicalRisk and UnsupportedOSRisk.

### UnsupportedOSRisk

This named group totals up the numeric values associated with an OS that is no longer supported. This is used in the TypeOfRisk named group. The formula used is:

**=SUM(VLOOKUP(INDIRECT("RC[-2]",0),RiskDetails,12,FALSE))**

#### Maintenance

This named group will only need to be updated if new columns are added on the Apps tab before L.

## Scorecard

The Scorecard tab is intended to provide an overview for each system along with a quick visual of the risk trend for each system. This tab does not provide information on why a system has the current score. This will likely be the only tab used by IT Governance, Corporate Compliance or the Board Audit Committee.

Applications are placed into one or more groups on this tab, those groups are:

* Mission Critical Applications
* Systems Accessible over the Internet (DMZ)
* Payment Card Industry (PCI) [Credit/Debit cards]
* Protected Health Information (PHI)
* Internet Hosted Applications (Cloud)
* Internal Systems without Patient Information or Credit/Debit Cards
* Uncategorized

The structure of each grouping is the same; the purpose of having different groups is that they may have different risk tolerances. This also helps visually show whether systems which are mission critical, in the DMZ, contain PHI or credit/debit information must have a green score.

### Structure

Most of this worksheet is generated dynamically; the only cell to change is column A. The value in column A will determine what shows up in all of the other columns.

There are six columns on the Scorecard tab:

* Application
* Risk Score
* Type of Risk
* Never Events
* Trend
* Description

The categories or groupings on this worksheet are: Mission Critical Applications, Systems Accessible over the Internet (DMZ), Payment Card Industry (PCI) [Credit/Debit Cards], Protected Health Information (PHI), Internet Hosted Applications (Cloud) and Internal Systems without Patient Information or Credit/Debit Cards

#### Application Name

The value entered in each cell of the Application Name column must match an entry on the Apps tab in column A. This is the key that will be used to dynamically populate other fields on the tab using VLOOKUP and INDIRECT formulas in the named group. Case does not matter but everything else in the cell does.

##### Formulas or Conditional Formatting

There are no formulas or conditional formatting in column A.

#### Risk Score

The risk score is entered through a VLOOKUP formula, based upon the value in column A of that same row. The score is calculated on the Apps tab and displayed here along with conditional formatting based upon the risk score value.

##### Formulas or Conditional Formatting

This cell uses the RiskScore named group

There are three conditional formatting rules for the Risk Score column which are applied to all cells in column B with the following line:

**=$B:$B**

###### Blank or Zero Values

If a cell is blank the conditional formatting removes any fill color. This was done because the range of cells where conditional formatting is applied should not be colored unless there is a numeric value. Without this in place there will be blank cells that are red.

###### 4,999 and Lower

Cells with a risk score below 5,000 are made green with conditional formatting.

###### 5,000 to 9,999

Cells with a risk score from 5,000 to 9,999 are made yellow with conditional formatting.

###### 10,000 and Higher

Cells with a risk score at 10,000 or above will be made red with conditional formatting.

#### Type of Risk

The Type of Risk column calculates any major areas of risk using the TypeOfRisk named group.

##### Formulas or Conditional Formatting

No additional formulas or conditional formatting are applied to values in this column.

#### NeverEvents

Never Events are things that should never happen, but when they do it may serve as a symptom of a larger problem. This field is populated using the NeverEvents named group to show when there is no documentation for a backup, no defined data classification and no assigned owner.

##### Formulas or Conditional Formatting

No additional formulas or conditional formatting are applied to values in this column.

#### Trend

The Trend column looks at the value in column A of the same row and then generates a Sparkline using data from the RiskTrend named group. All of the heavy work is done using the RiskTrend named group. If you copy that named group into the Sparkline source data range field it will not work properly because of the INDIRECT formula, this must be done by named group.

##### Formulas or Conditional Formatting

No additional formulas or conditional formatting are applied to values in this column.

#### Description

The Description column uses the AppDesc named group to pull the description in column C of the Apps tab into this column. An application can be listed multiple times so this ensures that the value only has to be entered in one location.

##### Formulas or Conditional Formatting

No additional formulas or conditional formatting are applied to values in this column.

#### Date

Cell A1 is updated with each release of the Risk Scorecard to have the date of release along with the Application Name column header.

## Apps

The Apps worksheet provides detailed information on why a given application has the current score. This worksheet will primarily be used by Application Analysts and is the only source of data for formulas; this is also the only page to be updated when generating a new scorecard. There is a column for the Application Name, Risk Score, Description Team and each item that will be measured.

Each column representing something to measure has a note in row 2 explaining why that item is being measured. Some of the columns have variable scores, for example not having a completed risk assessment for something which involves ePHI will increase the score by 10,000 points, however if the system lacks ePHI the increase will only be by 2,500.

##### Formulas or Conditional Formatting

There is only one formula on this worksheet which is used to total up the measured items. However data validation is used to restrict what values can be entered in most of the cells.

## Scoring

The Scoring worksheet is a static page to display what is being measured and when other things will be measured. This page is for reference.