

# Using the ITSM Metrics Modeling Tool

## *ITSM Metrics Model Tool Overview*

The ITSM Metrics Model is a simple spreadsheet tool that can be used for a variety of measurement and reporting purposes. The model can be used as:

- ✓ A starting point to identify key metrics that can be used to measure and monitor the health and state of your ITSM processes and activities
- ✓ Justifying an ITSM improvement initiative by modeling desired target future state improvements expected to occur
- ✓ A means for demonstrating the impacts and effects of current ITSM practices

- ✓ A means for modeling future business decisions to assess their impact and risk to ITSM activities if those decisions were to take place
- ✓ A means for modeling the breaking point at which the quality of ITSM practices becomes untenable.

In short, this tool may be used to support ITSM reporting and to model the impact of changes to the IT infrastructure or future business decisions.

## *Installing the Model*

The model is built as a Microsoft EXCEL Spreadsheet and is included on the CD with this book. Simply download or copy this file to a desired folder on your PC. The PC itself should be running WINDOWS XP or other platform compatible with Microsoft Office 2003.

It is recommended that you install the original version of the file and make changes only to copies of it. This will allow you to continually reuse the original to create baselines or future state models of your ITSM environment. For example:

1. Download and copy the original file to your PC as **ITSM Metrics Model.xls**
2. Create a baseline of your ITSM current state environment by making a copy of this file, applying your metrics results and storing it as **ServiceBaseline.xls** (for example)
3. Create state models of your future ITSM and business decisions by creating copies of your baseline model and storing it with some relevant name (i.e. **PostMerger.xls** for example) and then apply changes to that baseline. In this way, you can create multiple versions of models based on different business scenarios and compare their risks and impacts. There will be more on this later.

When you first use the model, the values that are in the Operational and Tolerances sections (colored Yellow) are arbitrary. These have been put in there for placeholders. You will be replacing these with your real results.

## *How to Use the ITSM Metrics Model Tool*

The model is simple to use. It consists of an EXCEL Workbook with individual Worksheets for each ITSM process plus Service Desk and Workforce Worksheets. A Dashboard Worksheet is also included that averages and summarizes the results of all the ITSM processes. For each Worksheet, the steps are:

- 1) Fill out the **Tolerances** section of each worksheet with your **Target** and **Warning** values for each Key Performance Indicator (KPI)
- 2) Fill out the **Operational Metrics** section of each worksheet with values from ITSM tools, reports and observations
- 3) Optionally, determine whether you want to skip a particular Worksheet by changing the **Activate This Model** box from **Yes** to **No**. If you make this change, the model will assume that you ARE NOT performing this process and will RAISE modeled risk levels accordingly
- 4) Optionally, determine whether you want to exclude the results of a particular Worksheet by changing the **Add Results to Dashboard** box from **Yes** to **No**. It is not recommended that this option be taken since it means the Dashboard results will no longer reflect ALL the ITSM processes. Use this option only if you insist. It is there only for some organizations that want to see certain processes or combinations of processes without taking a holistic view of ITSM.

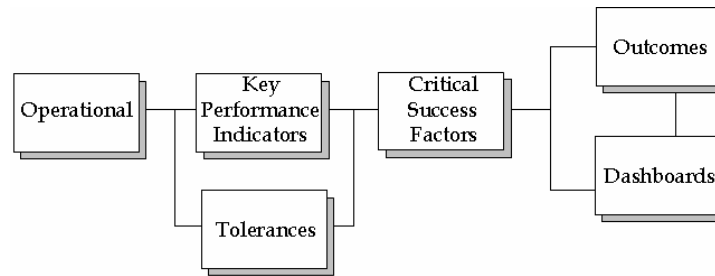
The model will automatically calculate the KPI values, compare them to the Tolerances and derive a LOW, MEDIUM or HIGH score with corresponding color (Green, Yellow, or Red) to indicate target status. A Green color indicates the KPI is at target or better. A Yellow color indicates the KPI is between the target and warning levels. A Red color indicates the target is above or below the warning level.

Critical Success Factors (CSFs) are automatically calculated based on the KPI values. A CSF consists of one or more KPIs that relate to it. It is color coded based on how well the combination of its KPIs were averaged. Therefore, a Red color indicates the CSF is at high risk, Yellow at Medium risk or Green at Low risk.

CSFs are then factored into the Worksheet level dashboard section. The balanced scorecard boxes (Customer, Capability, Operational, Financial and Regulatory) are derived from one or more combinations of CSFs that impact them. The same occurs with each of the operational risk areas (Legal Exposure, Service Outages, Rework, etc.). For these, the dashboard colors indicate the possible likelihood that exists for each risk occurring.

The Dashboard Worksheet is then calculated automatically as a rollup from each of the individual process dashboards.

The data flows within the model are fairly simple. It can best be described using the metrics model previously presented:



- 1) Tolerances are first entered for each process to describe acceptable and not acceptable KPI levels
- 2) Operational metrics are then entered for each process with live data from ITSM process reporting and other infrastructure measurements and observations
- 3) Key Performance Indicators (KPIs) are then calculated from the above and coded Green, Yellow or Red depending on how they fell within the specified Tolerance Levels
- 4) CSF risk levels are then calculated from combinations of KPI results and color coded as Green (Low), Yellow (Medium) or Red (High)
- 5) Each individual process Dashboard is then calculated from combinations of CSF results
- 6) The dashboard worksheet is calculated from averages across all CSFs and Dashboard risk results.

### *Interpreting the Model Results*

There are four items of interest that are output from this tool:

- ✓ KPI results
- ✓ CSF Results
- ✓ Balanced Scorecard Results
- ✓ Risk Assessment Results

#### KPI Results

These are the “Metrics That Matter”. An example from the Change Management worksheet in the model is shown below:

Key Performance Indicators (KPIs)		Question To Be Answered			
Change Efficiency Rate	95.0%	How efficient are we at handling changes?			
Change Success Rate	97.4%	How effective are we at handling changes?			
Emergency Change Rate	2.5%	What percentage of changes were emergencies?			
Change Reschedule Rate	5.0%	How well do we implement changes on schedule?			
Average Process Time Per Change (Days)	2.9	How long does the average change take?			
Unauthorized Change Rate	2.1%	What percentage of changes bypassed the Change process?			
Change Incident Rate	0.3%	What percentage of changes caused incidents?			
Change Labor Workforce Utilization	78.0%	How much available labor capacity was spent handling changes?			
Change Management Tooling Support Level	2.4	How well does our current tool set support Change Management activities?			
Change Management Process Maturity	2.4	How good is our Change Management practices?			

The results for each KPI are shown as calculated from the Operational Metrics input earlier. Color coding is based on how well the KPI fell within the Target and Warning Tolerance levels. Red results indicate potential areas that need to be improved.

As an example, the *Change Success Rate* KPI is calculated as follows from the Operational Metrics:

$$\text{Number of Failed Changes} / \text{Total Changes Implemented}$$

Therefore, if you implemented 1,000 changes and had no failures you scored a 100%. If you had 100 changes fail, you scored a 90%. This result is compared against what you input for Tolerance target and warning levels. If you indicated that your target was 98% and the warning level was 85% (as an example), then a 100% score would appear green. The 90% score would appear yellow. If your score ended up as, 84% for example, the score would appear red.

### CSF Results

These are derived from specific KPIs that relate to them. An example from the Change Management worksheet in the model is shown below:

Critical Success Factors	Target Level
Protect Services When Making Changes	High
Make Changes Quickly And Accurately In Line With Business Needs	Medium
Make Changes Efficiently And Effectively	High
Utilize A Repeatable Process For Handling Changes	Medium

In the above, “Protect Services When Making Changes” is calculated from the following KPIs:

- ✓ Emergency Change Rate
- ✓ Unauthorized Change Rate
- ✓ Change Incident Rate

These KPIs were chosen because they relate to specific threats to “Protecting Services When Making Changes”. The model examines each of those KPIs and then provides a result equal to the KPI with the highest risk. Therefore, for example, this result could score a Red (High) in the situation where a low Emergency and Unauthorized Change rate existed with a high Change Incident Rate.

Balanced Scorecard Results

A high level Balanced Scorecard is presented that looks like the following:

Customer	Capability	Operational	Financial	Regulatory
Medium	Medium	Medium	High	None
4.0	9.0	6.0	3.0	0.0
2	4	3	2	1

This is simply a showing of each scorecard area (Customer, Capability, Operational, Financial and Regulatory) with a color coded result that indicates the risk level for each area (Green (low), Yellow (medium), and Red (high)).

The first row of numbers underneath represents a calculated score total. This is taken from the mean average of all the CSFs that were input to that score. The second row simply indicates the number of CSFs that were used to calculate the score.

In the above example, the Capability Score is 9.0 and there were 4 CSFs that fell into that area. These values are used to determine the High, Medium or Low rating for the scorecard box. They are there only for calculation purposes.

Risk Assessment Results

Risk assessment results are also included with each Dashboard. These represent outcomes derived from the KPIs and CSFs. They are pictured as follows:

Low	➡	Legal Exposure	1.0	1
Low	➡	Service Outages	1.0	1
Medium	➡	Rework	4.0	2
Medium	➡	Waste	2.0	1
High	➡	Delayed Solutions	3.0	1
Medium	➡	Slow Operational Processes	2.0	1
None	➡	Security Breaches	0.0	1
None	➡	Inaccurate Information	0.0	1
High	➡	Slow Turnaround Times	3.0	1
Medium	➡	Unexpected Costs	9.0	4
Medium	➡	Higher or escalating costs	8.0	3
Low	➡	Low Employee Morale	1.0	1
High	➡	Slow Response To Business Needs And Changes	3.0	1
Low	➡	Unwanted PR Exposure	1.0	1
Medium	➡	Dissatisfied Customers	4.0	2
None	➡	Dissatisfied Suppliers	0.0	1
Medium	➡	Inability to scale	5.0	2
Medium	➡	Fines and Penalties	4.0	2
Low	➡	High Levels Of Non-Value Labor	3.0	2
Medium	➡	Loss of Market Share	4.0	2
Medium	➡	Loss of Revenue/Sales	6.0	3

Each risk area represents a possible outcome based on how well CSFs were met. The color coded box to the left of each outcome indicates the likelihood that the associated risk might occur.

The number values to the right of each risk are similar to the dashboard results except they are specific to each risk. These are used to calculate the High, Medium, Low rating and color for each risk identified.

## *Modeling Business Decisions*

One of the main purposes of the tool is to model the impact of business decisions or ITSM improvements that you are thinking about or planning to make. Examples of questions you may be trying to answer might be as follows:

- ✓ What will be the impact on our IT service quality if we put a major new application into production?
- ✓ How much operational risk will occur if we go through with a planned merger or acquisition?
- ✓ Which ITSM improvement initiatives will provide us with the most benefit?
- ✓ How many problems, incidents or changes can we handle before the quality of our services breaks down?
- ✓ What is the impact of increasing our Change Management CMMI Process Maturity from 2.4 to 3.5?

If using the tool to model things like this, you will first create a Baseline ITSM Model. The Baseline will represent your Current State practices. This model will be populated with the results of the way you currently utilize ITSM processes and activities. In this, you will populate the Tolerances and Operational Metrics as described earlier.

The next step is to create a series of Future State ITSM Models. These are also known as “What-If” Models. For each of these models you will make a replica of your baseline model and then make various changes to it that reflect various scenarios that you would like to model.

As an example, let's say that most of your ITSM Processes are at a 2.0 level. What might be the impact if you raise this level to 3.0? For this, you would:

- 1) Make a replica of your baseline ITSM model
- 2) Change the Process Maturity to 3.0 in the Operational Metrics section of each process you are interested in
- 3) View the results

You could then save this model for future reference and build other models to reflect other scenarios such as:

- ✓ What happens if the volumes of Incidents are decreased by 20%?
- ✓ What happens if the Emergency Change rate rises by 30%?
- ✓ What happens if Change Management labor is decreased by 10%?

Remember that only the Operational Metrics will be changed for What-If models. The model will calculate whether those changes resulted in KPIs that fell out of (or into) desired Tolerance levels.