SOX (Sarbanes-Oxley) Plugin

The Sarbanes-Oxley Act is a landmark piece of US securities legislation affecting corporate governance and financial disclosure. In order to comply with the requirements, business process flows must be instrumented with information that allows for compliance analysis.

What is the SOX plugin?

The SOX plugin is comprised of an Inspector view, a set of definition editors and a report writer which outputs a compliance report into Microsoft Excel.

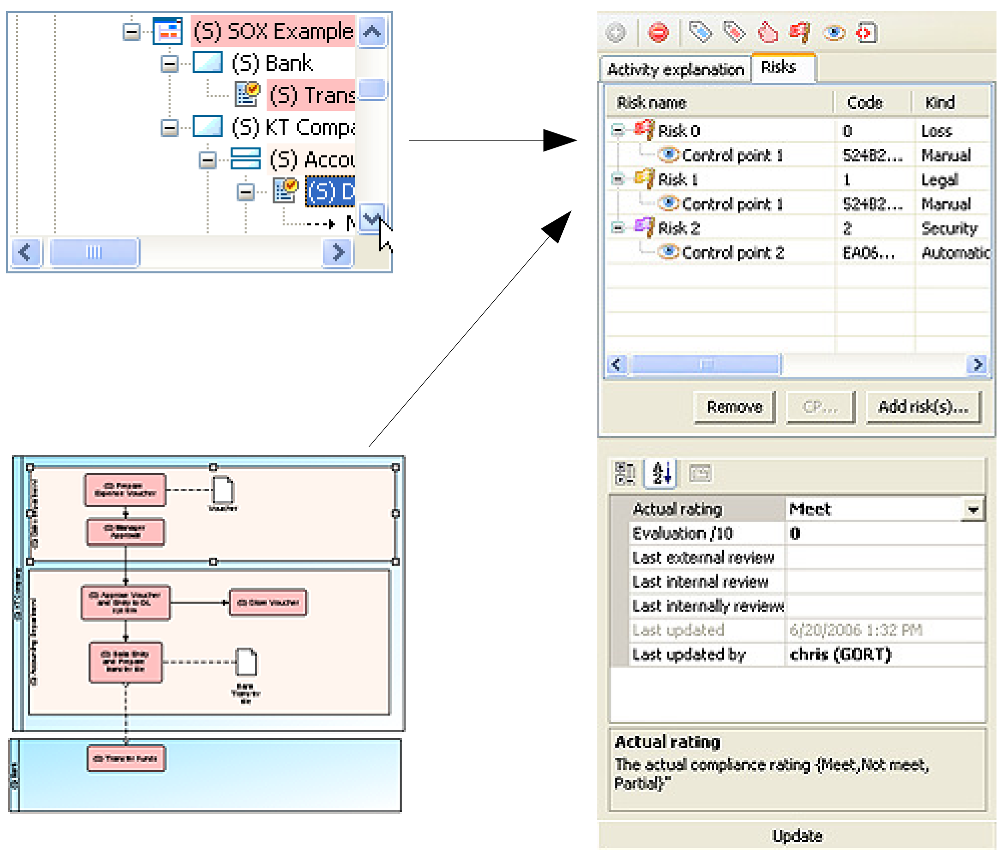
Using the inspector you can add and edit SOX information to the process model.

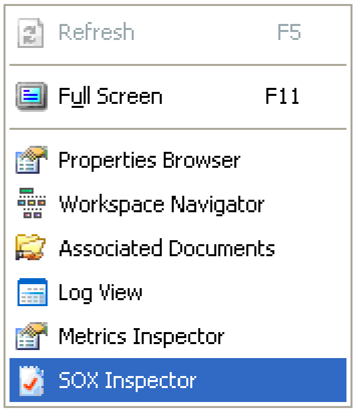
When you make a selection in the Diagram Editor or the Workspace Navigator, the SOX inspector displays any SOX information which may be attached to the selected object.

You can operate the SOX plugin with or without the use of the diagram editor.

Information added with the inspector becomes part of the process model and is saved with your process model when it is saved.

The SOX plugin is an add-on to Avantage that provides a set of tools to instrument a BPMN process model with SOX compliance and control information.



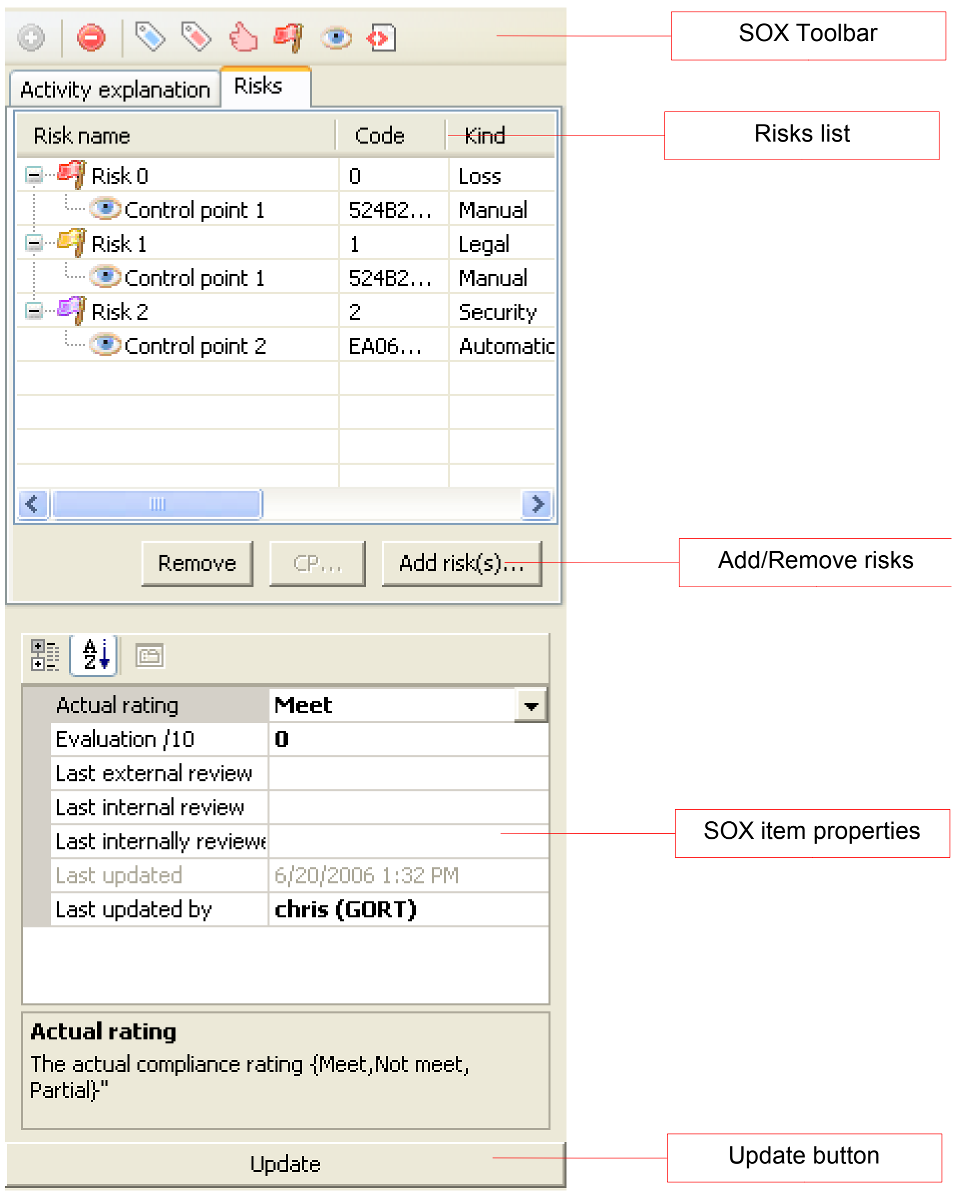


The SOX Inspector

The SOX Inspector is made visible by choosing the **SOX Inspector** menu item from the **View** menu.

Note: If this menu is not present in your computer it means that the SOX Plugin is not installed.

Figure 1. The SOX Inspector view

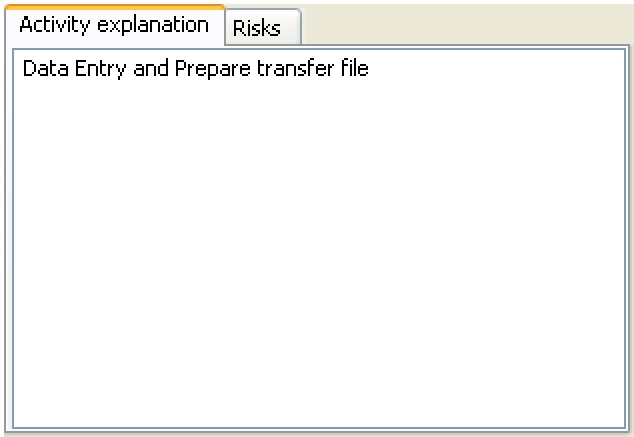


The Activity Explanation tab

This tab initially displays the BPMN object's caption. You can add extra text here to describe in more detail the nature of the activity.

Note: The plugin does not allow this field to be blank. If you clear the text it is automatically reset to the name of the BPMN object it is associated with.

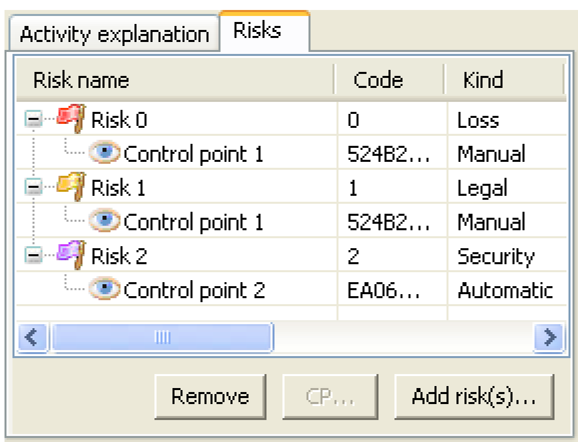
Figure 2. The activity explanation tab



The Risks Tab

This tab displays the Risks associated with the selected BPMN process entity. You can add and remove risks using the "**Add risks...**" and "**Remove risk**" buttons.

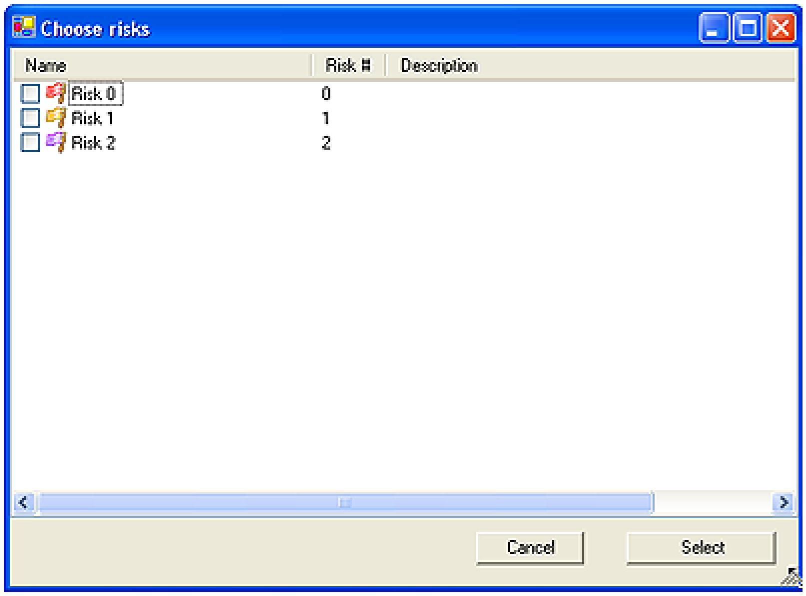
Figure 3. The Risks tab



Adding a Risk

To add a risk, click the "Add risk(s)" button. This will display the risk picker dialog. If the Risk you assigned includes control point definitions then they too will be displayed in the risk list (as children of the risk). These "designed-in" control points cannot be removed from the Risk instance.

Figure 4. The risk picker dialog



The risk picker dialog shows all of the currently defined risks. You can select one or more risks to be added to the SOX item by checking their appropriate checkboxes.

Removing a risk or Control Point

Select the item in SOX inspector and then click the Remove risk button. You can remove a control point if it is not designed-in to the Risk in the Risk editor.

Adding a Control Point

By clicking on the "CP.." button you can assign arbitrary control points from the control points table to a Risk instance.

The SOX item properties

For each BPMN object to which you attach SOX instrumentation, a packet of data is created. This packet of information is saved in a named BPMN property in the form of an Xml encoded string. The following properties describe the SOX item as a whole.

Actual rating

This is a rating that is assigned to the item when it is reviewed. The plugin provides some basic pre-defined ratings (Meet, Partial, Not meet). You can define additional ratings using the Ratings editor.

Evaluation score (/10)

An over-all rating number in the range of {0..10} is assigned to the item.

Last external review

This is the date that the control was last reviewed by an external accredited reviewer.

Last internal review

This is the date that the control was last reviewed by an authorized staff member.

Last internally reviewed by

This is the identification of the internal reviewer. It can be a employee number, initials, an email address, system username etc.

Last updated

This is the date and time that the SOX item was last updated back into the process model. This field is automatically stamped when you click the SOX Inspector's "Update" button.

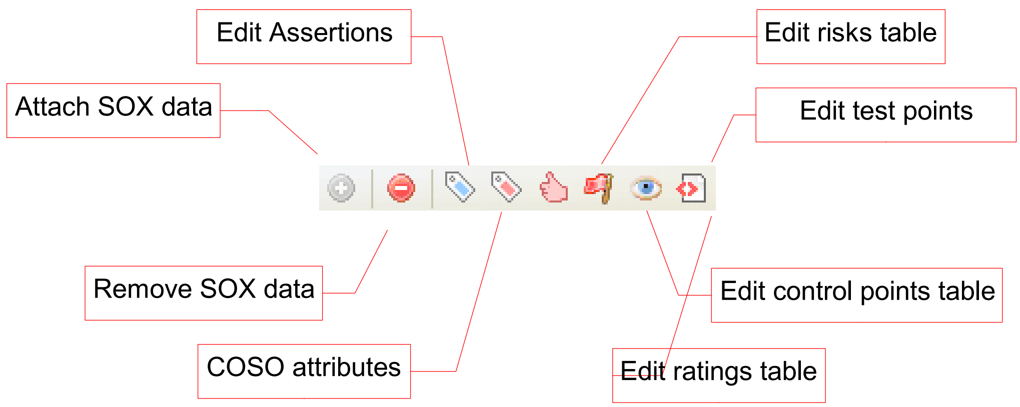
Last updated by

This is the Windows username and domain of the person who is running the Avantage session. This field is automatically stamped, in the format of **`username (domain)`**

Using the SOX Plugin

SOX control information be added to Diagrams, Pools, Swimlanes, Tasks and SubProcess objects. The SOX inspector panel is blank when you select an object that is not a candidate for SOX control.

Figure 5. The SOX Inspector toolbar



To attach SOX data to a BPMN object

If the selected BPMN object doesn't have any SOX control information the "**Attach SOX data**" toolbar button is enabled. When you click this button the object becomes SOX enabled.

To remove the SOX data from an object

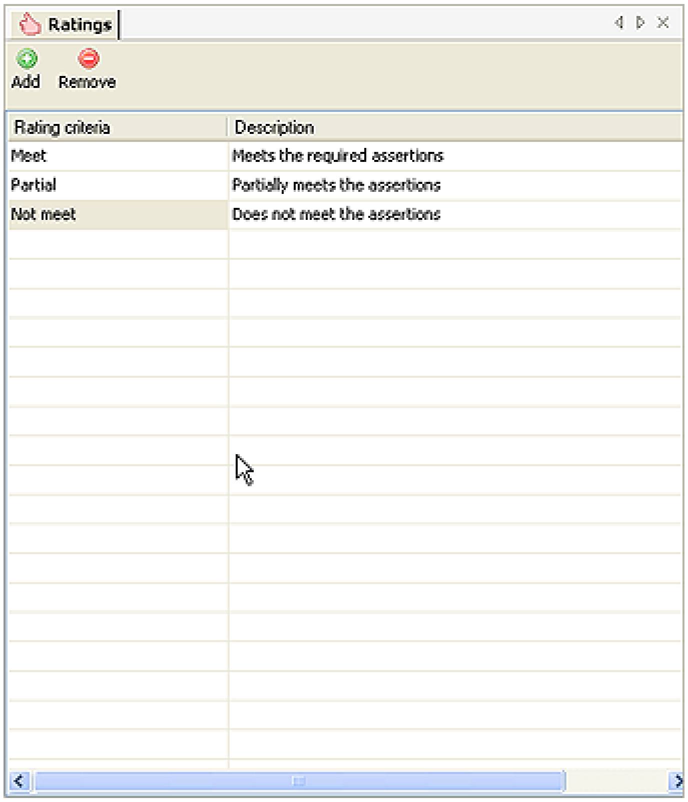
To remove the SOX record from the object click the "**Remove SOX data**" toolbar button.

The Update button

Clicking the Update button updates the BPMN process object with the data that you entered with the inspector. Unless you click the Update button the data will not be permanently associated with the process model.

The Ratings Editor

Figure 6. The Ratings table editor



By default there are three pre-defined ratings (Meet, Partial and Not meet).

You can add your own additional ratings.

The Excel report generator checks for the pre-defined ratings and colors rating cells accordingly. If you alter or delete these three items then coloring no longer applies.

Add

Click the "**Add**" button.

Remove

Select the rating line and then click the "**Remove**" button.

To edit

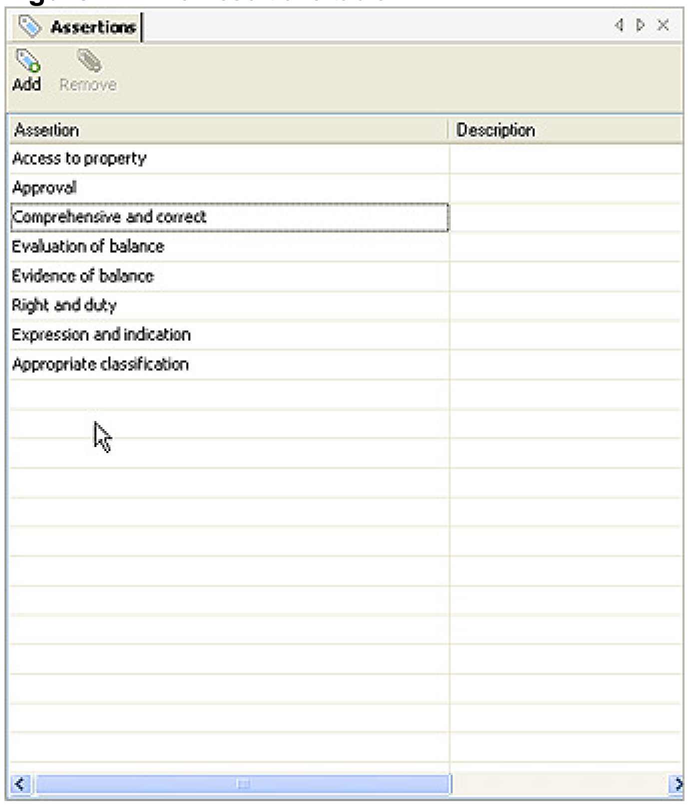
Double-click the cell and directly enter the text into the cell.

Save

Choose the File Save menu, Control-S, or click Yes to the prompt when you close the editor.

The Assertions Editor

Figure 7. The Assertions table



Assertions are associated with Risks and form the basis of the criteria by which a Risk is measured.

Add

Click the "**Add**" button.

Remove

Select the criteria line and then click the "**Remove**" button.

To edit

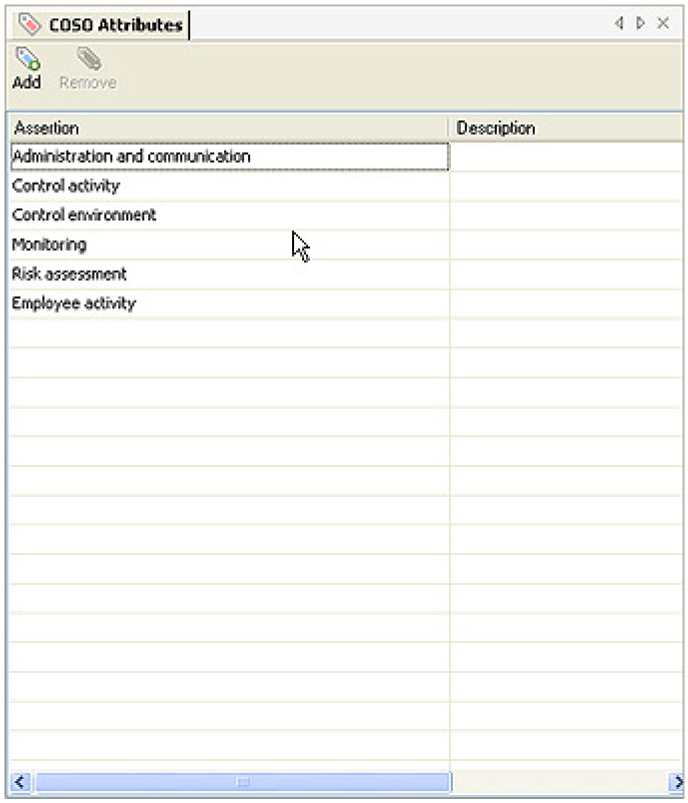
Double-click the cell and directly enter the text into the cell.

Save

Choose the File Save menu, Control-S, or click Yes to the prompt when you close the editor.

The COSO Attributes Editor

Figure 8. The COSO table editor



COSO attributes are associated with Control Points and indicate the criteria a Control Point is managing.

Add

Click the "**Add**" button.

Remove

Select the criteria line and then click the "**Remove**" button.

To edit

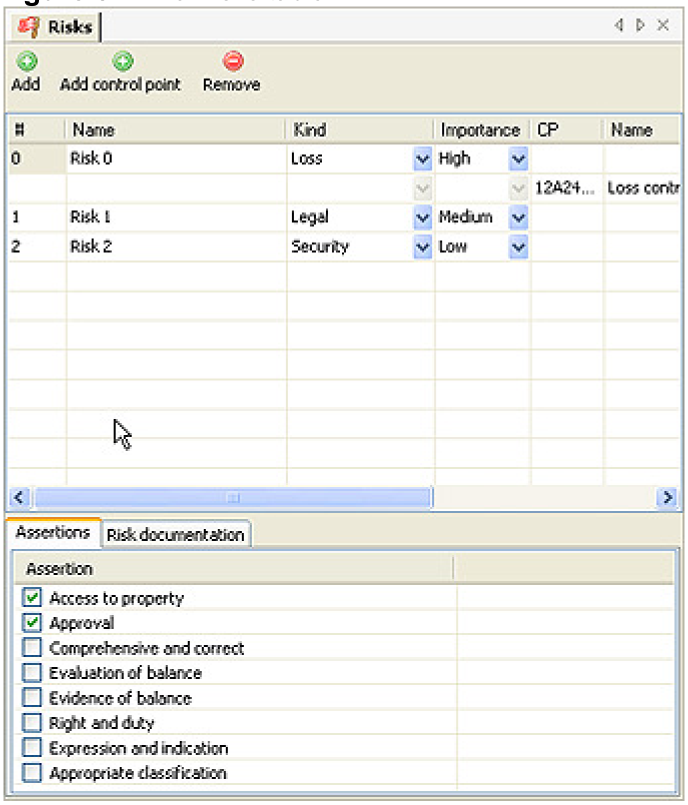
Double-click the cell and directly enter the text into the cell.

Save

Choose the File Save menu, Control-S, or click Yes to the prompt when you close the editor.

The Risks Editor

Figure 9. The Risks table



The Risks editor is used to define risks. For each risk there can be a corresponding set of Control points which dictate how the risk is managed.

***Assertions**: By checking an assertion you add that assertion to the selected Risk. By un-checking an assertion you remove it from the Risk.*

Assertions are defined by the Assertions editor.

There are two sections to the risk editor. The top section displays the current set of Risks and their ControlPoints. The botton section displays the Assertions and documention related to the selected risk.

Add

Click the "**Add**" button to add a new Risk to the risks table.

Add Control Point

When a Risk is selected, clicking the "**Add control point**" button will display a dialog box which allows you to choose one or more Control points from the Control points table. The selected control point(s) are added to the table as sub-entries of the selected risk.

Remove

When a Control point is selected, Remove will delete the control point from the risk. If a Risk is selected, the Risk is deleted (and all of its Control Point sub-entries).

Kind

The Kind drop-down contains a list of pre-defined Risk kinds.

Importance

The importance drop-down contains a list of pre-defined importances (High, Medium, Low).

Description

Add a short text entry here to describe the risk. This description will appear in the SOX report. To add detailed descriptions use the Documentation panel of the editor.

To edit

Double-click the cell and directly enter the text into the cell. You cannot make changes to the Control Point entries (you should use the Control Point editor) to do that.

Save

Choose the File Save menu, Control-S, or click Yes to the prompt when you close the editor.

Documentation

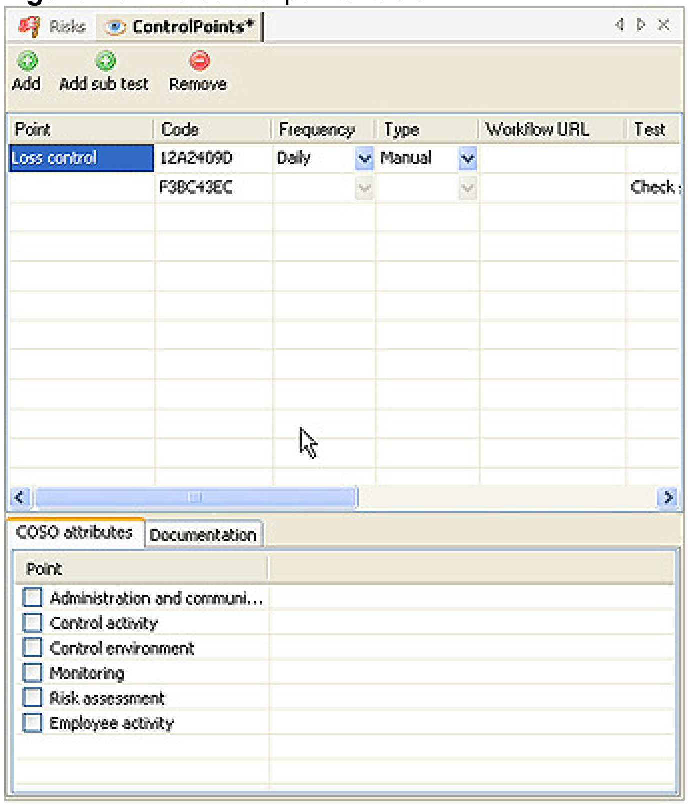
The documentation pane is RTF (Rich Text Format) text which can contain formatting and hyper links. You can paste formatted text from Microsoft Word, Open Office or any other RTF capable application into this field.

To enter a hyper link just enter the URL directly into the text. The text is automatically underlined and made into an active link. You can then click on the link to open that link in your web browser.

For example, you might enter here a link to the company policy for a particular Risk.

The Control Points Editor

Figure 10. The control points table



The Control Points editor is used to define control points. For each Control point there can be a corresponding set of Test points which dictate how the Control Point is managed.

***COSO Attributes**: By checking an attribute you add that attribute to the selected Control Point. By un-checking an attribute you remove it from the Control Point.*

COSO attributes are defined by the COSO attributes editor.

The control points editor allows you to create and modify structured control points. Control points can be associated with one or more Test Points.

Add

Click the "**Add**" button. A new structured note is created.

Add Test point

A main point must be selected first, then by clicking the "Add test point" button a Test Point dialog is displayed from which you can choose one or more tests. The selected tests are added underneath the selected main point as sub-entries.

Remove

Select the point and then click the "**Remove**" button. If the selected item is a Test point then it is removed. If the selected line is a main point it is removed as is all of its Test points.

To edit

Double-click the cell and directly enter the text into the cell.

Save

Choose the File Save menu, Control-S, or click Yes to the prompt when you close the editor.

Control Point properties

Point

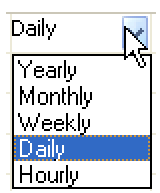
This is the name of the Control Point.

Code

This is a string that can be used to uniquely identify the control point. By default the SOX plugin will automatically insert a unique code here but you can change it if you want to because the code value is not used by the plugin. You can use it for any purpose in your SOX project. For example the code could be a query or a database search field.

Note: *The plugin doesn't enforce uniqueness of this code but the initial code generated by the plugin is unique.*

Frequency



Select a frequency from the drop-down list.

Note: If your frequency is not in the list just enter it directly into the field as text.

Type

The control point can be either manual or automatic. If the process is automatic a workflow process is used to perform the control.

Workflow URL

For automatic control points, this field represents the workflow process which performs the control.

Test

A control point may have a number tests associated with it. This property contains the name of each test.

Description

A short description of the control point. This description appears in the SOX matrix report.

Documentation

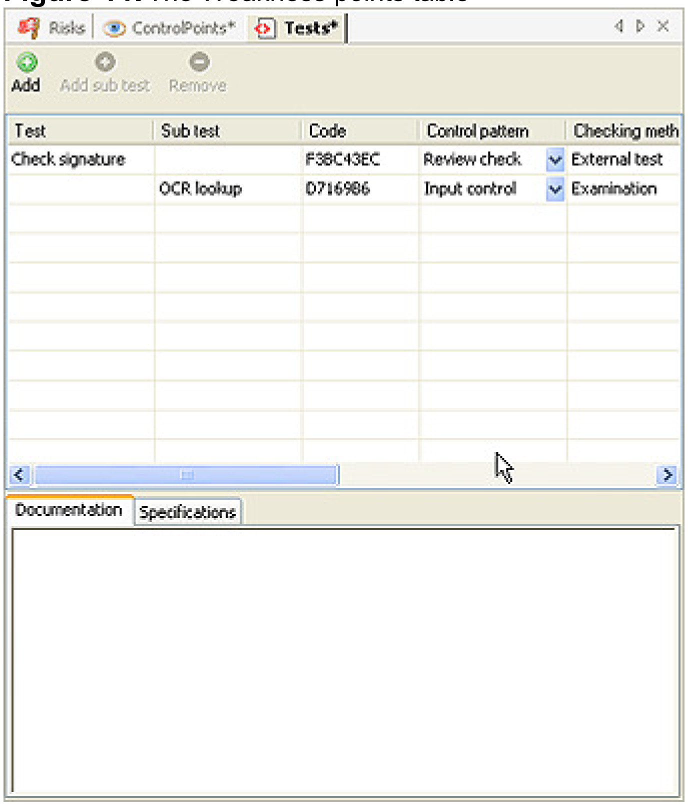
The documentation pane is RTF (Rich Text Format) text which can contain formatting and hyperlinks. You can paste formatted text from Microsoft Word, Open Office or other RTF aware application into this field.

To enter a hyperlink just enter the URL directly into the text. The text is automatically underlined and made into an active link. You can then click on the link to open that link in your web browser.

For example, you might enter here a link to the company policy for a particular Control Point.

The Test points Editor

Figure 11. The Weakness points table



The Test points editor allows you to create and modify test points. Test points are two level entries consisting of a "Test" and any number of "Sub tests". Tests and Sub tests have unique codes which enable them to be related with external entities.

Add

Click the "**Add**" button. A new test step is added.

Add sub point

A main test point must be selected first, then by clicking the "Add sub point" button a new sub test is added underneath the selected main test point.

Remove

Select the point and then click the "**Remove**" button. If the selected item is a sub test then it is removed. If the selected line is a main test it is removed as is all of its sub points.

To edit

Double-click the cell and directly enter the text into the cell.

Save

Choose the File Save menu, Control-S, or click Yes to the prompt when you close the editor.

Test Point properties

Test

This is the name of the test. For example "Test 1".

Sub Test

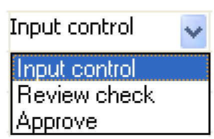
This the the name of a sub test, for example "Step 1".

Code

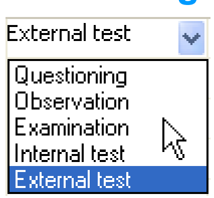
***Note**: The plugin doesn't enforce uniqueness of this code but the initial code generated by the plugin is unique.*

This is a string that can be used to uniquely identify the item. By default the SOX plugin will automatically insert a unique code here but you can change it if you want to because the code value is not used by the plugin. You can use it for any purpose in your SOX project. For example the code could be a query or a database search field.

Control pattern



Checking method



Sample count

This property is the number of representative samples on which the test is applied.

Description

A short description of the test. This information will appear in the Excel matrix report.

Documentation

RTF format text which can contain detail about the test or hyperlinks to URLs or documents that describe the test.

Specifications

RTF format text. If the test is technical in nature either the specifications themselves or a link to them can be placed here.

Producing a Compliance Matrix

A Compliance Matrix is a report that is created in Microsoft Excel. In order to produce a compliance matrix you need to have Excel 10 (Office XP) or later installed on your computer.

Choosing what to report on

***Note**: The report writer drills down into the process model from the current selection.*

Only BPMN objects that contain SOX data are included in the report.

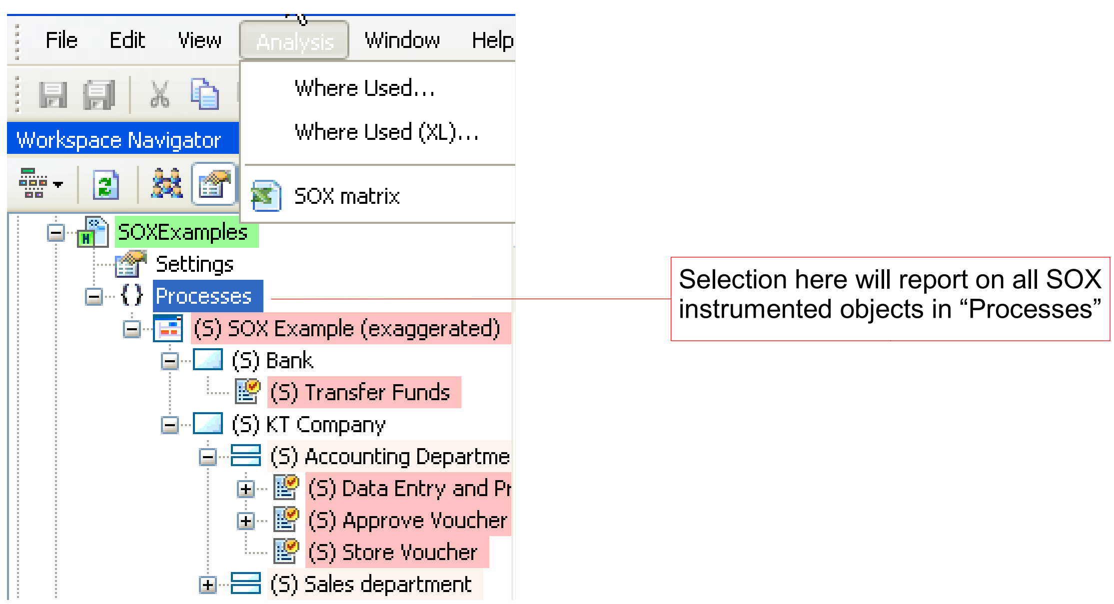
BPMN container objects (like Diagram, Pool, Lane, SubProcess) which directly or indirectly contain an instrumented BPMN object are displayed in the matrix using a Container Break entry in the matrix. You can change the appearance of Container Breaks with the Preferences page settings.

The **Analysis:SOX matrix** menu on the main menu bar is enabled whenever you select a BPMN object which contains SOX control information.

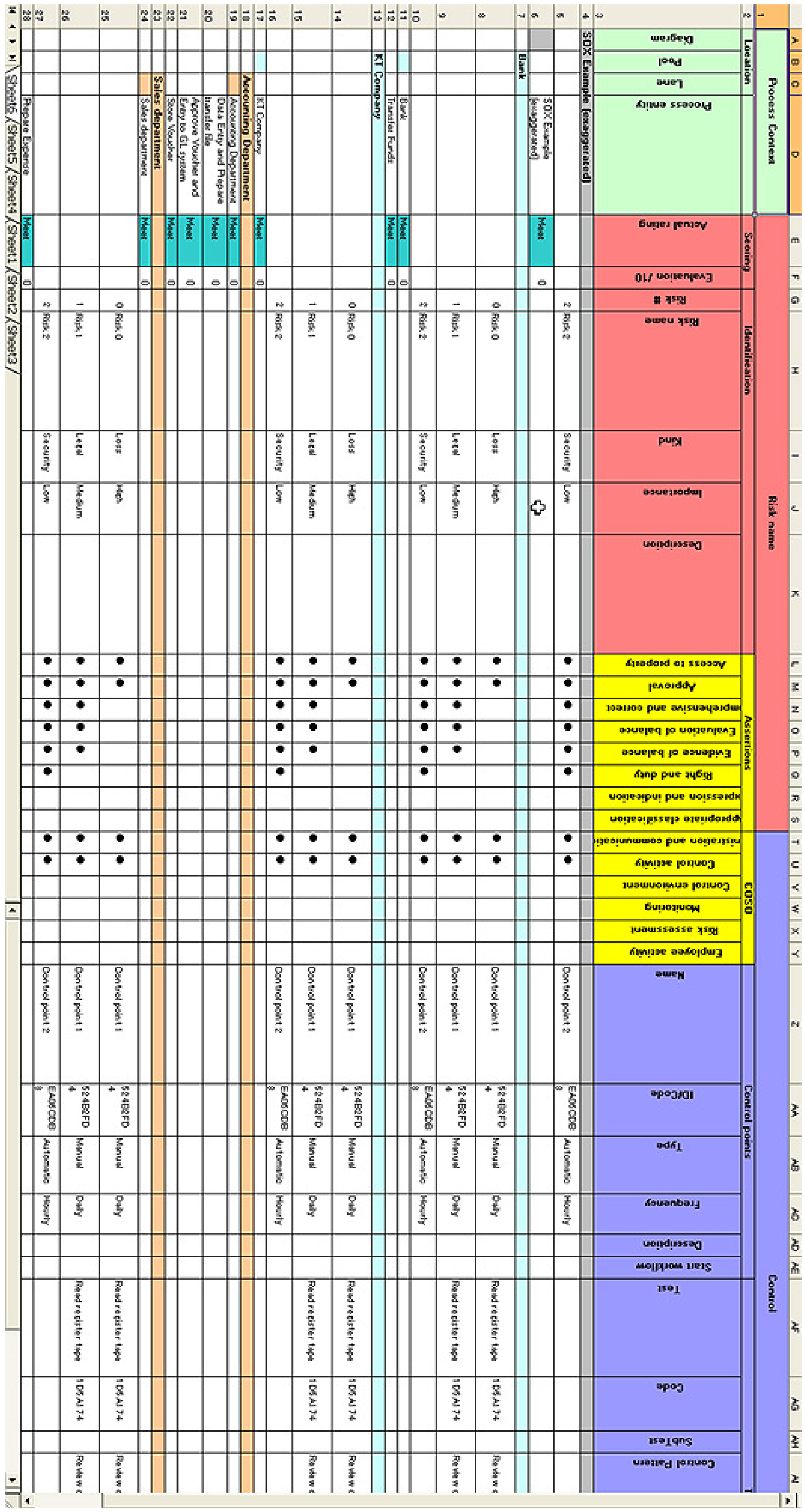
It is best to make the selection from the Navigator tree rather than from a diagram editor window. This is because you will often need to make a report from a higher level object than a BP diagram (for example you might want to produce a SOX matrix for the entire process model, or you might want to report on all the diagrams in the "To be" measurepoint – you cannot do that by selecting things from inside a diagram editor window).

The SOX Report menu can be enabled when the current selection is either a Model (.model) file, a MeasurePoint, a Diagram, a Pool, a Swimlane, a SubProcess or a Task.

The menu is grey (disabled) unless the selected object itself contains SOX information or one of its child objects does.



The report writer outputs directly into Microsoft Excel (so it is necessary for Excel to be installed). Each report creates a new Worksheet in the Excel workbook each time you run the SOX matrix action.



Definition files

The plugin is designed to allow you to start using it immediately with no special setup required. If you plan to use the plugin in a team/workgroup environment then a little extra bit of setup is required.

Personal workspace definitions

***Note**: You will need to set your folder options to Display Hidden Files and Folders in order to see these files.*

It is recommended that you always use project based definitions since this allows you to keep the definitions together with your project and they can be backed up together.

By default, the plugin creates a set of definition files in your *personal* workspace storage. For example, a user named "chris" will have his personal items stored here:

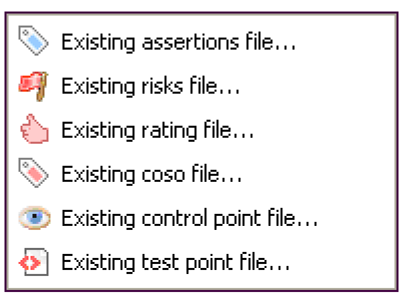
```
C:\Documents and Settings\chris\Application
Data\Kaisha-Tec\Avantage\Plugins\KT.AM.SOXC
```

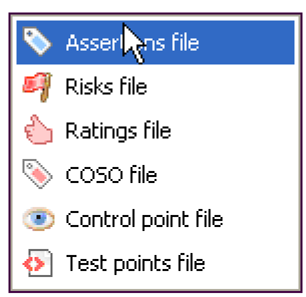
The definitions in your personal workspace will be used for all of your projects unless over-ridden on a project by project basis.

If you are working in a team or in any way planning to share your SOX process model with other people then it is necessary for all team members to work with the same definitions, in which case you must put the definitions into the project itself (so that they can be managed by the repository).

Project based definitions

You can create new definition files or add existing definition files by right-clicking on the project's icon in the workspace navigator and choosing either the **New** or **Add** actions.

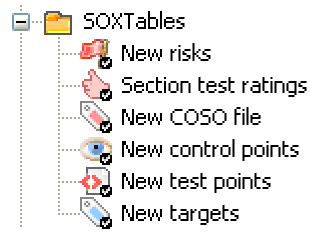




The Add command will prompt you for an existing file which will be copied from its location. You can copy your personal definition files into a project this way. The New command on the other hand, creates a completely new file.

Figure 12. Definition files are stored in the project's workspace

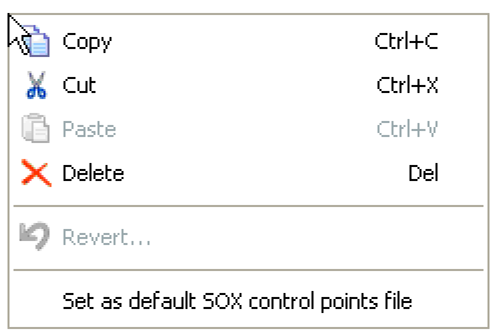
***Note**: It is a good idea to put all of your definition files into their own dedicated folder in your project as this minimizes visual clutter.*



Forcing Avantage to use your project based definitions.

It is not sufficient to just place a definition file in the project in order for it to be used. You must specifically tell Avantage which files are to be used as the default files for the project. This is done by right clicking on the definition file and choosing the “Set as default” action.

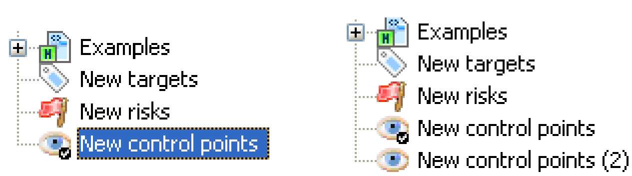
Figure 13. The Set as default action



After selecting this action the file's icon is drawn with a special marker (a tick) to indicate that it is now the default file of this type within the project.

If you have multiple files of the same type this action lets you switch between defaults. For example, you could have an experimental file and a production file.

Figure 14. Definition file showing a default marker



The SOX plugin will use this definition file whenever it is operating on any process model within this project instead of using your personal definition.

You can turn the default property OFF by right-clicking on a default item and then choosing the “**Remove as default**” action.

Decorators – visually indicating the SOX items in a diagram

You can choose a special label ***Prefix*** and background colors for SOX instrumented BPMN objects. This makes it easy to identify them at a glance in process diagrams and the Navigator.

You can specify separate indicator colors for Pools, Lanes, SubProcess and Task objects. By default indicator colors are not enabled (they are set to transparent).

To change the Label Prefix and indicator colors edit those so named properties in the SOX Preferences page.

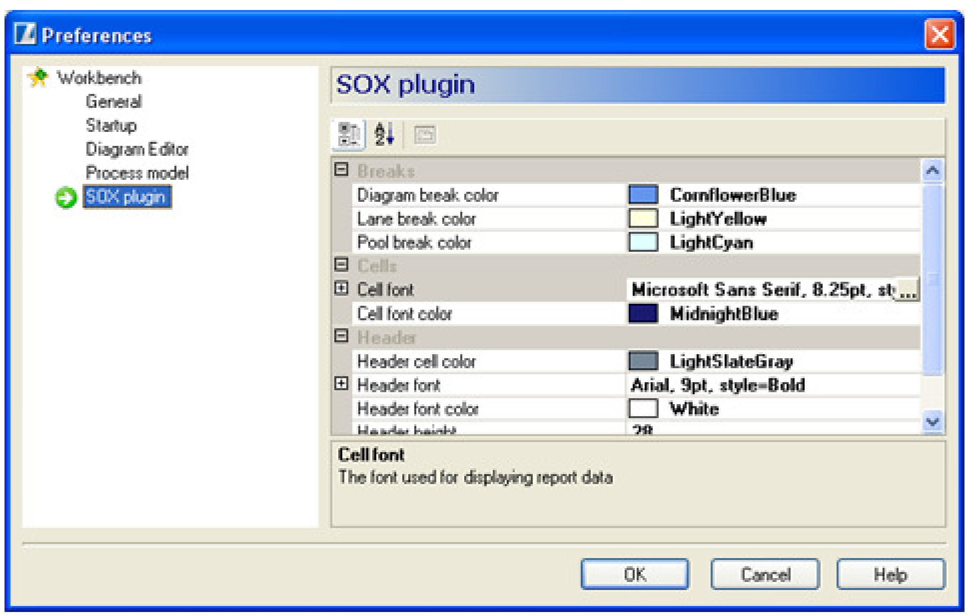
The default label prefix is **(S)** .

To disable an indicator color effect set it to ***Transparent***.

Plugin Preferences

Select the Preferences item from the File menu and then click on the SOX plugin entry in the preferences list.

Figure 15. The SOX Preferences page



These settings allow you to change default fonts, colors and other formatting information used in producing a report.

Under the hood

SOX data are attached to BPObjects in the process model with BPMN Property objects of type ***string*** which contains Xml encoded data representing the objects in the SOXPlugin's space.

Figure 16. How SOX data relates to the BPMN process model