Security Compliance Manager

User Manual – Draft

Version 0.5.1
2006-05-26

Disclaimer
This is a proof-of-concept prototype application built as part of a doctoral dissertation project submitted at the Institute of Information Systems, Department of Information Engineering at the University of Bern, Switzerland. Although I put considerable effort into the creation of the software and its documentation, I cannot guarantee for its correctness. Due to its nature as a proof-of-concept prototype, the software is not intended to be used in a production environment. Therefore, you must use it *at your own risk* or *not use it at all.* *Martin Luethi, San Francisco, 05/25/06*

Table of Contents

1 Introduction

Security Compliance Manager (SCMA) is a graphical proof-of-concept modeling application prototype that supports information security management activities in health care organizations. It allows easy drag-and-drop modeling capabilities for heterogeneous and distributed information system architectures. Additionally, their security compliance can be analyzed against various predefined and custom security policies. The model consists of nodes (e.g., symbolizing information, application, and system elements) and edges that connect the nodes (e.g., symbolizing data flow between systems, applications, and information; or indicating mapping relationships). The model is intended to provide a simplified management level perspective, not an accurate technical view.

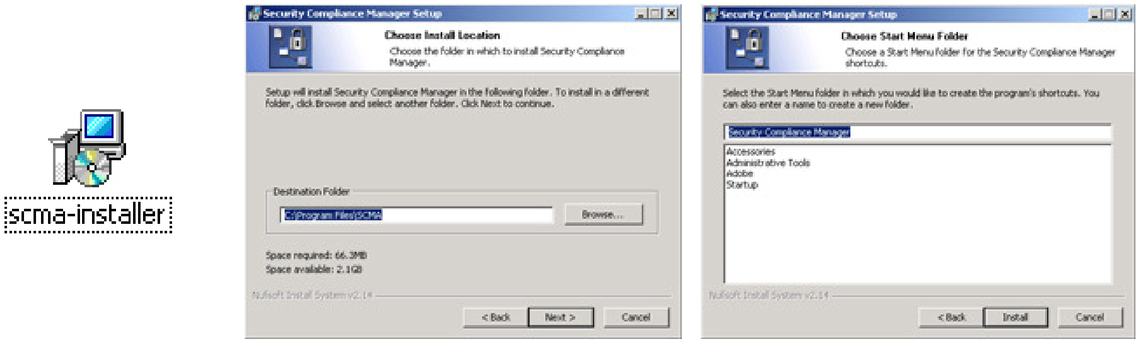
The application is an academic prototype, which focuses especially on including the connectedness of nodes for an assessment of the security compliance. In contemporary compliance assessments these connections are often neglected. However, in particular in a fragmented environment that requires a certain subset of information to comply with regulation, the relatedness of nodes is considered important. The software at hand is a proof-of-concept thereof. Although attributes of nodes have to be entered manually and picked from customizable option lists, in a production-grade application these attributes would be imported from existing software agents directly (as available from many system monitoring tool vendors) or selected from corporate data repositories and directories. Such interfaces can be implemented easily but are outside the scope of this work.

2 Installation

SCMA is written in Java and can be run platform independently. For Windows users, the application is packaged in a standard Windows installer file, which does not require any additional software or JRE to be installed. It can be downloaded and run from:

`http://www.luethi.net/download/scma/scma-installer.exe`[1]

Setup is simple and started by double-clicking `scma-installer.exe`. The entire process is self explanatory and installs the application including a private JRE into the chosen directory. Application and installer have been tested on Windows 2000 and XP.



Security Compliance Manager Setup

Choose Install Location

Choose the folder in which to install Security Compliance Manager.

Setup will install Security Compliance Manager in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Program Files\SCMA

Space required: 66.3MB

Space available: 2.1GB

Security Compliance Manager Setup

Choose Start Menu Folder

Choose a Start Menu folder for the Security Compliance Manager shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

Security Compliance Manager

Accessories
Administrative Tools
Adobe
Startup

Figure 1: Windows installation process.

[1] As of version 0.5.0, the total installation file size for Windows is 25.3MB.

The following directory structure will be created under the chosen installation location:

Directory	Description
SCMA/	
data/	XML options, mapping, policies, and user manual
lib/	External Java libraries
images/	Images and icons
jre/	Java Runtime Environment
samples/	Sample file directory
scma.exe	Executable program file

Table 2-1: Directory structure.

Four sample policies are provided with the application and are loaded automatically. The policies can be modified or additional policies can be added but are required to comply with the format used for the available policies. Moreover, new files need to be indexed in `index.xml`. The following policy files are available out-of-the-box:

Directory	Description
./data/	
policies/	
hipaa.xml	HIPAA Security Standard
iso.xml	ISO-17799:2005
nist.xml	NIST/FISMA
vdsg.xml	Verordnung Datenschutzgesetz

Table 2-2: Pre-defined policy files.

For a quick introduction to the capabilities of the application, a sample data file is installed and can be loaded from the following location:

Directory	Description
./samples/	
simple-example.xml	Example data file with several pre-defined nodes and edges. Can be loaded and modified in order to get an overview of application capabilities.

Table 2-3: Sample file.

The application can be run from the command line. However, it requires a correctly setup Sun JRE 1.5, including the `JAVA_HOME` variable may need to be set. SCMA has been tested on Linux (Fedora and SUSE), Solaris, and Mac OS X. It can be downloaded at:

```
http://www.luethi.net/download/scma/scma.tar.gz
```

The file can be extracted and run with the following or similar commands:

```
gzip -d scma.tar.gz
tar -xof scma.tar
java -jar scma.jar
```

3 Modeling

SCMA features several standard application components. The menu bar provides the ability to navigate through all the functions of the application. The tool bar, which is separated into groups, provides short cuts to often used features and capabilities. The modeling pane is the graphical view where the drag-and-drop modeling occurs, it is separated by two lines (separator), which are explained below. The status bar provides the user with feedback about actions such as the selection of elements in the pane.

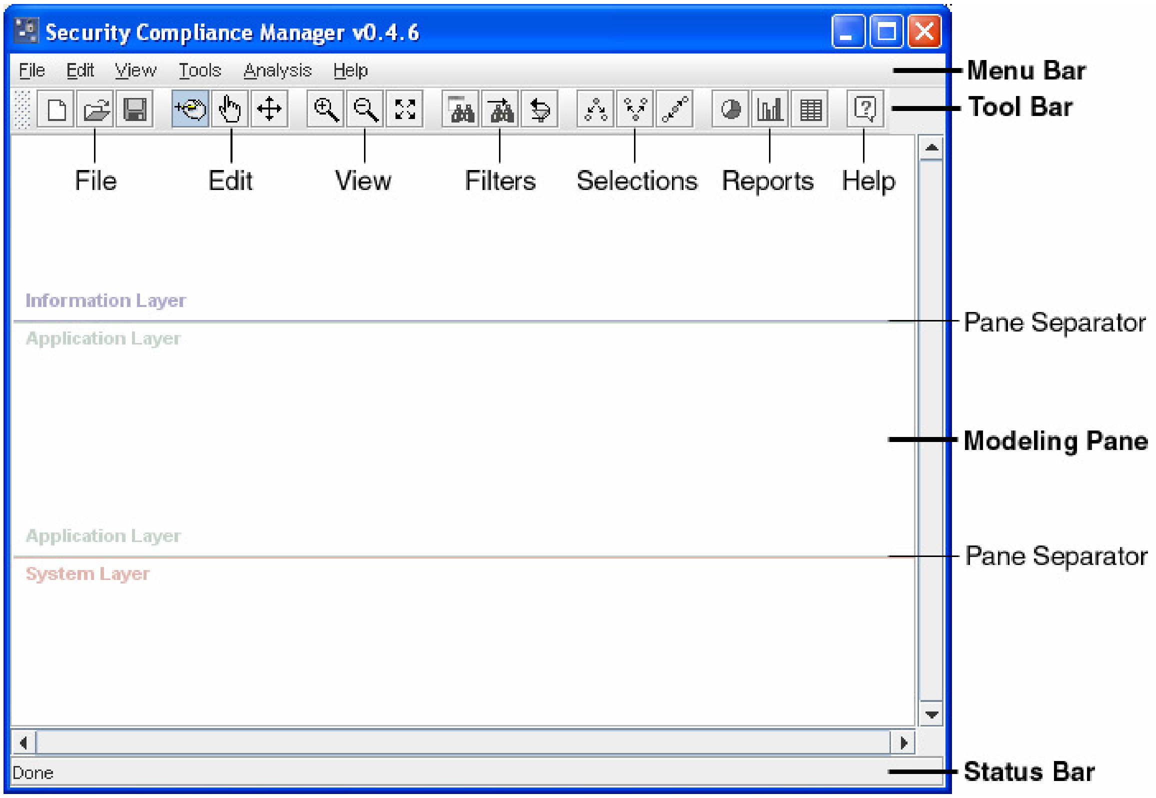


Figure 2: Security Compliance Manager application window.

The modeling activity can be started on an empty modeling pane or a previously created model. It can be loaded by using the `Open` 📂 icon on the tool bar or the menu bar using `File/Open`. By default, the `sample/` directory's location is used by the file dialog.

3.1 Tool Bar

The tool bar allows the user to select certain modes of operation or invoke one-time actions. It changes the behavior of the mouse in the modeling pane, changes its view, or brings up a dialog. The subsequent table summarizes the actions and comments their use.

File		
🗋	`New`	Drops the current and model and resets the modeling pane.
📂	`Open`	Opens a file dialog to retrieve a model file.
💾	`Save`	Stores the current model, prompts for a file name if it is a new file.

Edit		
	Editing	Left click on the edit pane creates a new node. Left click on an existing node brings up the node's property dialog. Left click on an existing node, holding down the mouse button, and dragging to another node creates a new edge. Right click on the editor field brings up the context menu. Right click on an existing node brings up the node's context menu.
	Picking	Left click on an existing node selects the node (enlarges icon). Left click on the edit pane and dragging marks a group of nodes. Dragging a selected node moves the node to a different location. Right click on an existing node brings up the node's context menu.
	Panning	Dragging moves the entire pane; scroll bars are provided if necessary. Especially useful after zooming the view, which allows to adjust it using the panning mode.

View		
	Zoom In	A left click on zoom in (+) zooms the view by 10%.
	Zoom Out	A left click on zoom out (-) zooms out the view by 10%.
	Resize View	Left click resets the zoom and position to its initial value.

Filters		
	Find Nodes	Opens a dialog to filter nodes by specific criteria.
	Find Edges	Opens a dialog to filter edges by specific criteria.
	Reset Filters	Resets all the filters and show all nodes and edges.

Selections		
	Show Successors	Requires one selected node, shows all its directly and indirectly succeeding nodes. All other nodes and edges are hidden.
	Show Predecessors	Requires one selected node, shows all its directly and indirectly preceding nodes. All other nodes and edges are hidden.
	Show Neighbors	Requires one selected node, shows all its directly connected nodes. All other nodes and edges are hidden.

Reports		
	Information System Summary Report	Invokes a report presenting the static structure of the entire health information system. Proportions of nodes and edges by type, ownership, as well as a list of nodes counting their selected attributes are provided.
	Information Security Configuration Report	Brings up a static report of the security relevant attributes of all the nodes and edges. Lists policy compliance per node type, authentication, authorization, and recovery methods. Lists the attributes by node type.
	Sub-Graph Compliance Report	Requires one node to be selected. Calculates compliance values for all its succeeding nodes including an accumulated value that represents the total compliance value of the selected sub-graph.

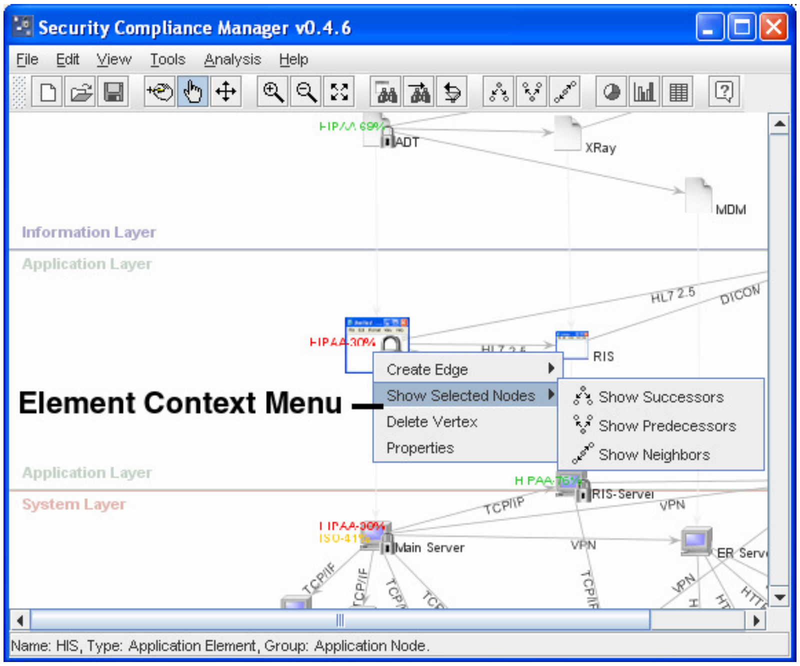
Help		
?	Help	Brings up this user manual in a separate dialog window. Requires a PDF reader application to be installed to work properly.

Table 3-1: Tool bar items and their function.

Some actions can also be found in the menu bar. Operation modes can only be selected on the tool bar, however. The menu bar can be detached from the window by dragging.[2]

3.2 Modeling Pane

To display an abstract management view of the entire health information system, SCMA features three node types and four edge types. Each node represents either an information, application, or system element. Edges one-directionally connect two nodes together and represent information, application, or system flows, or mapping relationships. Further, each node or edge can have a defined number of attributes, which can be selected from an option list or can be added freely.



Name: HIS, Type: Application Element, Group: Application Node.

Figure 3: Element context menu.

The attributes further determine how the elements are treated during the analysis process. Node and edge attributes can be attached by bringing up the an element's context menu. This can be achieved by two ways. First, in editing mode a node can be selected by pressing the left mouse button and the property dialog will open up directly. Second, in picking mode an element has to be selected and the right mouse button makes the context menu appear. When `Properties` is selected the property dialog appears.

3.2.1 Nodes

The three different node types are listed in the table below. The type a node is associated with is determined at creation time and cannot be changed, it depends on the mouse position when creating a node. In the modeling pane, generally, there are two separation lines visible, which indicated in what area which node type will be created. Subsequent

[2] It can be reset to the original position by closing the detached window.

movement of a node outside its area does not change its type. To change a type, a node has to be deleted and a new node needs to be created inside its determined area.

Information Node		
📄	Information Node	They symbolize information or, loosely speaking, documents and are associated with business processes (function), business units (unit), and information elements (data).
🗔	Application Node	They symbolize applications that are used to process the information elements. They are associated with data elements (data), roles (role), and vendors (vendor).
🖥	System Node	They are actual physical computer systems used to run and use the applications and process the information elements. Typical fields are location, vendor, operating system, network, etc.

Table 3-2: Node types.

Each node type can hold several attribute values. The key/value pairs do have a one-to-one cardinality, meaning that the node can only be associated with one `owner` for example. Some attributes allow the association with multiple values, such as `unit` for instance. Internally the values are stored as strings and can therefore assume any format.

Node Properties	📄	🗔	🖥		
Name	•	•	•	1:1	Node name that is displayed by default on the modeling pane.
Owner	•	•	•	1:1	Associated owner who is responsible for the node.
Group	•	•	•	1:n	Assignable arbitrary label to allow operations on a subset of nodes.
Unit	•			1:n	Unit reading and writing information nodes.
Function	•			1:n	Functions producing and consuming information.
Data	•			1:n	Data fields/elements belonging to the element.
Role		•		1:n	User role implemented in application.
System		•		1:n	Application system type.
Vendor		•	•	1:1	Vendor of application or system.
Version		•	•	1:1	Version/Product name of application or system.
Location			•	1:1	Physical location of system.
OS			•	1:1	Operating system of computing device.
IP			•	1:1	IP address of computing device.
Net			•	1:1	Subnet/network of computing device.

Table 3-3: Node properties.

Where it makes sense, an attribute has an option list which allows the user to select one or multiple values. The option lists are customizable and can be adjusted to the system environment. Security properties work in the same way as node properties. They are used for the security analysis of the health information system. The following security properties can be specified for each node type:

Security Properties	📄	🗔	🖥		
Target	•	•	•	1:1	Security target consists of assigned values for confidentiality, integrity, availability, and

					accountability. Each attribute can assume `none`, `low`, `medium`, or `high` as a value.
`Policy`	•	•	•	1:n	Predefined security policy applicable to node.
`Authentication`		•	•	1:n	Used authentication controls.
`Authorization`		•	•	1:n	Used authorization controls.
`Auditing`		•	•	1:n	Applied auditing controls.
`Recovery`		•	•	1:n	Associated recovery plans.
`Software`			•	1:1	Security software such as AV, patch mgmt, etc.

Table 3-4: Security properties.

Although the attributes cannot be changed during runtime, the application has been written to allow easy addition of more attributes. However, this requires access to the source code and requires recompilation.

3.2.2 Edges

Several types of edges are supported, primarily determined by the nodes they connect. Generally they can be differentiated between flow and mapping edges. Flow edges can be of three different types as listed in the table below. Mapping relations connect two different kind of nodes and indicate how the node of the upper layer is implemented.

Edges	
`Information Flow`	A connection between two information nodes, symbolizing the flow of information without making any assumption of its implementation.
`Application Flow`	A data flow between two applications, determining the protocol how the data flow is realized on the application layer.
`System Flow`	A connection between two system nodes, indicating how the data flow is actually implemented on the system layer.
`Mapping`	A mapping relation that shows what lower layer elements are actually used by nodes above in the information system.

Table 3-5: Edge types.

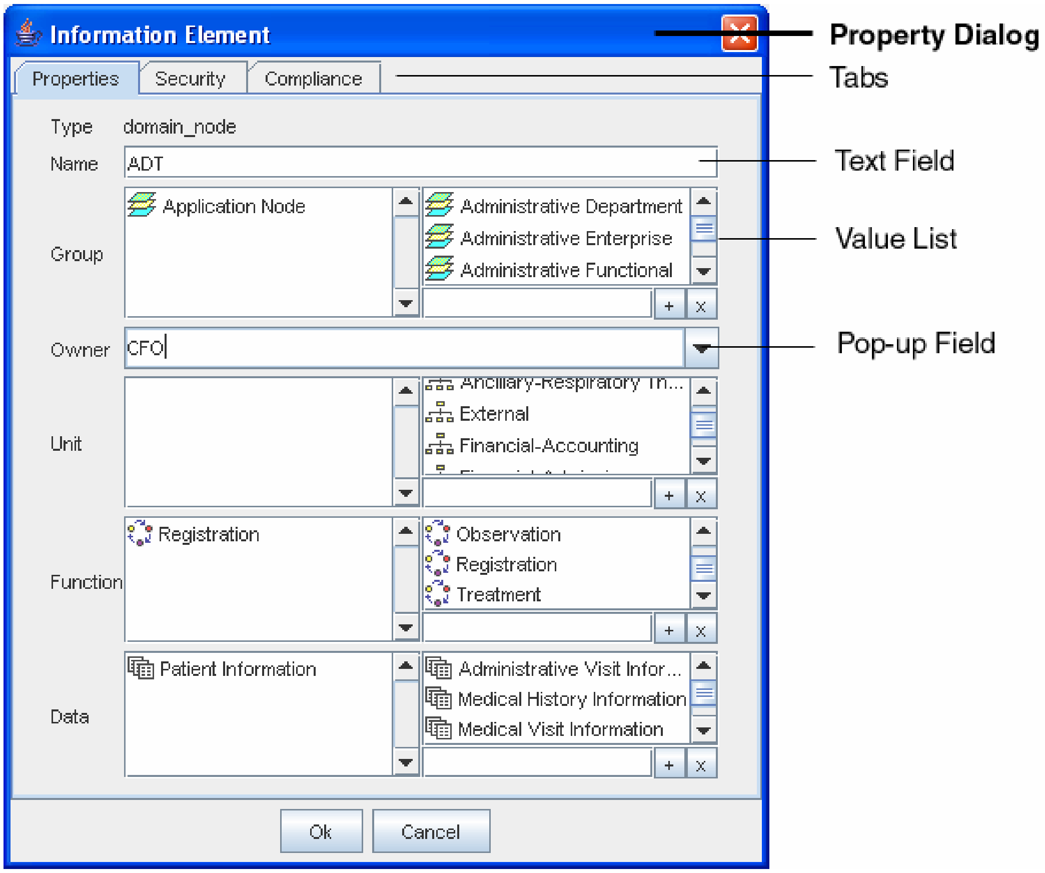
Corresponding to nodes, edges can assume attributes. The following edge attributes all have a one-to-one cardinality and can be assigned using an edge's context menu.

Edge Properties					
`Name`	•	•	•	1:1	Edge name, which can be displayed on modeling pane.
`PHI`	•			1:1	Boolean value, which indicates that protected health information is transmitted via this edge.
`PII`	•			1:1	Boolean value, which indicates that personally identifiable information is transmitted.
`Protocol`		•	•	1:1	Protocol that is used to transmit the data.
`Encryption`			•	1:1	Boolean value, which indicates if the data transmitted is encrypted.

Table 3-6: Edge properties.

3.3 Property Dialog

Each element type has its own property dialog, showing its specific attributes only. The dialogs are organized in the same manner. They contain three tabbed panes that can be switched by pressing a tab. Each tab contains several attribute fields as described in 3.2.1 and 3.2.2. Modifications on all the three panes are committed or canceled simultaneously by pressing the corresponding button. Below the different attribute type fields are explained in more detail.



Type domain_node

Name ADT

Group: Application Node | Administrative Department, Administrative Enterprise, Administrative Functional

Owner CFO

Unit: | Ancillary-Respiratory In..., External, Financial-Accounting

Function: Registration | Observation, Registration, Treatment

Data: Patient Information | Administrative Visit Infor..., Medical History Information, Medical Visit Information

Figure 4: Information element property dialog.

3.3.1 Text Field

A text field is a one line text area, which can hold a string of various length. It does not provide any optional choices or remember any entered values. It is primarily used for naming of nodes, products, etc. Each element can only hold one value per attribute (1:1).

Name ADT

Figure 5: Text field.

3.3.2 Checkbox Field

The checkbox field contains a Boolean value, which indicates if a condition or statement is true or false (i.e., yes or no) for a specific element attribute.

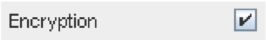


Figure 6: Checkbox field.

3.3.3 Pop-up Field

Pop-up fields or combo boxes allow the selection of exactly one value out of a predefined but customizable list. The option list is kept in a separate XML file and is therefore remembered for other nodes or models. Also, if the corresponding choice for an attribute value cannot be found in the list, the cursor can be set onto the text area and the value can be entered by keyboard. It is immediately added as an option to the list and will appear the next time in the list. Each element can only hold one value per attribute (1:1).

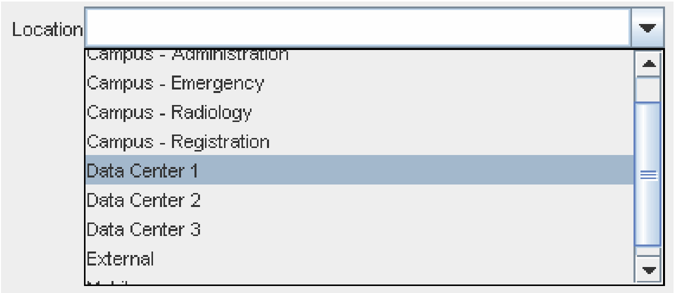


Figure 7: Pop-up field.

3.3.4 Slider Field

The slider field allows the selection of a numerical value out of a predefined range. This field type is currently used for the selection of the security target, which is expressed as a scale-like value, assuming values between `Low` and `High`. Additionally, the most left position of the slider indicates `None` as a security target. Internally, the selection is handled numerically as a choice between the range of 0 to 3. The slider does not record any options and also allows only one value per attribute.

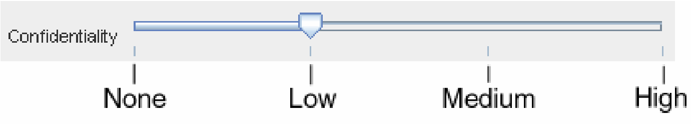


Figure 8: Slider field.

3.3.5 Value List

The value list is similar to the pop-up field but allows multiple selections per field. A selection can be made by a left click on an entry of the `Option List`. The entry immediately appears on the `Selection List`. If an option is not listed it can be added by typing its value into the `Edit Field` beneath the `Option List`. It can be added by pressing the `Add Button` or removed by using the `Remove Button`. Options are stored independently of the model and are remembered for each element of this or any other model. Each element can hold multiple values per attribute (1:n).

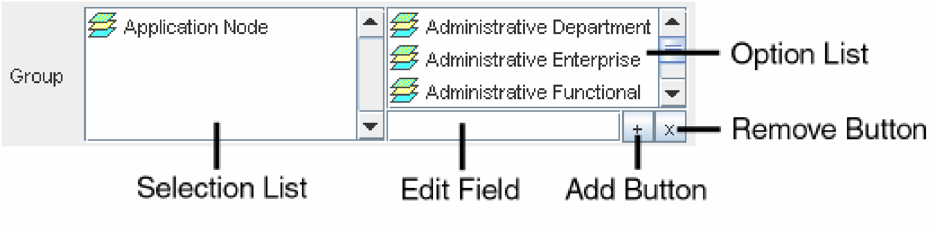


Figure 9: Value list.

3.3.6 Compliance List

A compliance list is used to represent security policies. Each node can have several security policies assigned, which are selected using a regular `value list`. However, since every security policy can contain several control categories and control items expressing the compliance with items, another form of representation is required. The compliance list is organized in a folder structure allowing unfolding and folding of control categories. Control items can be checked, indicating their compliance, or unchecked symbolizing non-compliance. Each policy can contain unlimited numbers of control categories and control items. Categories can contain other categories. A policy structure is defined within an XML policy file as listed in Table 2-2.

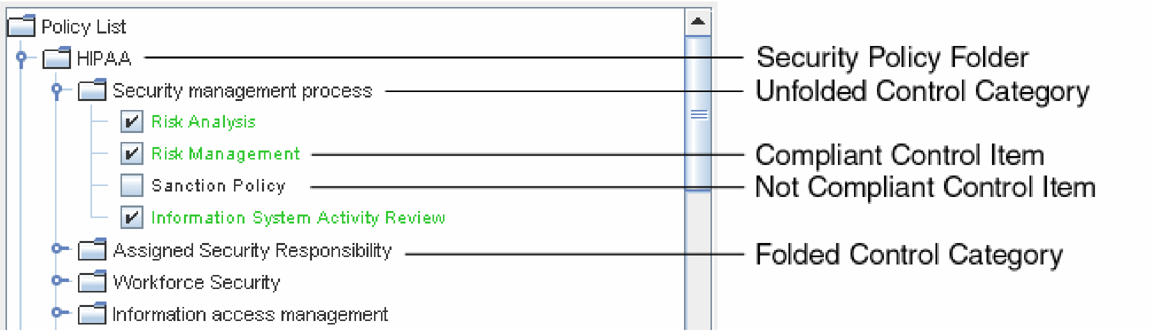

Policy List
HIPAA
Security management process
☑ Risk Analysis
☑ Risk Management
□ Sanction Policy
☑ Information System Activity Review
Assigned Security Responsibility
Workforce Security
Information access management
Security Policy Folder
Unfolded Control Category
Compliant Control Item
Not Compliant Control Item
Folded Control Category

Figure 10: Compliance list.

4 View and Tools

This section describes the functions found in the `View` and `Tools` menu. Views include filters that can be applied to show a subset of all nodes and edges. Labels determine the text that is presented next to each element on the modeling pane. The selection can be made via checkboxes, which allow multiple values to be selected at the same time. Radio buttons are exclusive and only one selection can be made at a time.

4.1 Nodes

4.1.1 Selection

A node can be selected by pressing the left mouse button on a desired object. The selection operation is indicated by the magnification of the node icon. Several nodes can be selected simultaneously and the editing operations apply to all selected nodes. The nodes can be unselected by pressing an empty area on the modeling pane.

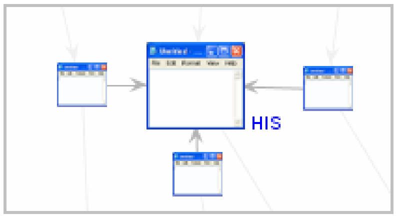
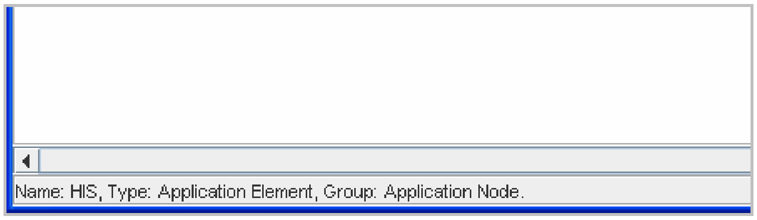


Figure 11: Selected node.

Simultaneously some attributes of the selected node are presented in the status bar at the bottom of the screen. They currently include the element's name, its type, and its groups.

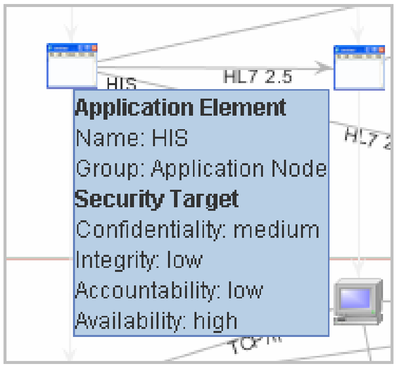


Name: HIS, Type: Application Element, Group: Application Node.

Figure 12: Status bar, showing attributes of selected node.

4.1.2 Tool Tip

When hovering the mouse pointer over a node or edge for a few seconds, the element's tool tip appears. It is a short description of the element including its name, owner, group, and security targets. If an attribute is empty it will not appear in the description.



Application Element
Name: HIS
Group: Application Node
Security Target
Confidentiality: medium
Integrity: low
Accountability: low
Availability: high

Figure 13: Tool tip.

4.1.3 Status

Applied node policies appear on the modeling pane in form of an overlaid lock icon. Additionally, the name of each applied policy including its compliance status is presented on the pane. The compliance status is expressed in percentage and calculated by dividing the compliant control items by the number of the total items for the policy. Moreover, the status is emphasized by color codes (green >= 66%, 66% > yellow > 33%, red =< 33%).

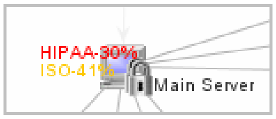


Figure 14: Policy indicator.

4.2 Filters

Filters allow to hide a subset of nodes. They remain active until another filter is applied or the `Reset Filter` action is executed. Alternatively, an empty area on the modeling pane can be clicked once. The filters can be combined and are applied together.

Filters			☑	●	
	`Node Filter`	`Domain nodes`	•		Hides information nodes if unchecked.
		`Logical nodes`	•		Hides application nodes if unchecked.
		`Physical nodes`	•		Hides system nodes if unchecked.
	`Edge Filter`	`Flow edge`	•		Hides all flows connecting nodes on the same layer if unchecked.
		`Mapping edge`	•		Hides mapping edges if unchecked.
	`Security Filter`	`All`		•	Shows nodes with all security targets.
		`Confidentiality m/h`		•	Shows nodes with at least a medium confidentiality security target.
		`Integrity m/h`		•	Shows nodes with at least a medium integrity security target.
		`Availability m/h`		•	Shows nodes with at least a medium availability security target.
		`Accountability m/h`		•	Shows nodes with at least a medium accountability security target.
	`Reset Filter`				Resets the filters to default (all nodes and edges are visible).

Table 4-1: Filters.

4.3 Labels

Labels are presented next to each element on the modeling pane. The default labels shown for nodes are `name` and for edges `protocol`. If these attributes do not have any values assigned, they will show up empty.

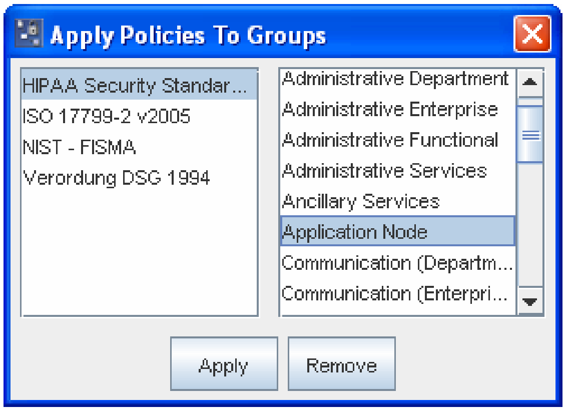
Labels			☑	●	
	`Node Labels`	`Name`		•	Node name, blank if empty.
		`Type`		•	Node type: domain, logical, or physical node.
		`Location`		•	Node location (system nodes only), blank if empty.
		`Owner`		•	Node owner, blank if empty.
		`Degree`		•	Incoming and outgoing connections.
		`None`		•	No label.
	`Edge Labels`	`Protocol`		•	Protocol of connection (application and system flow only).
		`Name`		•	Name of connection.
		`Type`		•	Edge type: domain, logical, physical

		flow or mapping.
	Weight	• One divided by the total number of outgoing connections.
	None	• No label.
Reset Labels		Resets the label setting to default (name and protocol labels are visible).

Table 4-2: Labels.

4.4 Apply Policies to Groups

Each created node by default belongs to one group depending on its type, which is either `Information Node`, `Application Node`, or `System Node` group. However, each node can belong to an arbitrary number of additional groups. The group attribute is useful to batch apply certain functions to a subset of nodes simultaneously. For instance, the `Apply Policies to Groups` function allows to apply or remove policies to multiple nodes using one operation. For example, to apply the HIPAA security policy to all application nodes, the policy can be selected in the left list, whereas the applicable groups are selected in the right list. Multiple policies and groups can be selected by holding down the `shift` key. In that case the operation is performed using a logical `OR` operation. Pressing the `Apply` or `Remove` button performs the operation.



Apply Policies To Groups

HIPAA Security Standar...
ISO 17799-2 v2005
NIST - FISMA
Verordung DSG 1994

Administrative Department
Administrative Enterprise
Administrative Functional
Administrative Services
Ancillary Services
Application Node
Communication (Departm...
Communication (Enterpri...

Figure 15: Apply policies to groups dialog.

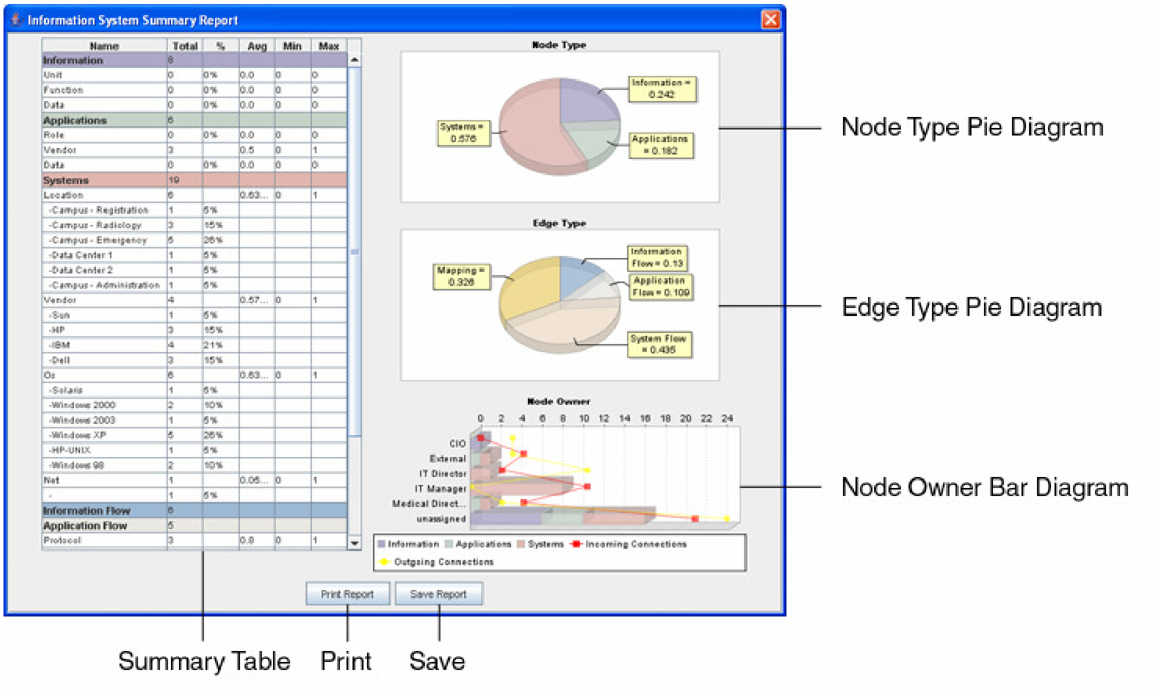
5 Reports

Reporting is a key component of the application. Generally there are two different types of reports: first, static reports that indicate the status of the entire system and do not require the selection of any specific node. Second, reports that are intended to provide information regarding one specific node including relevant data of its connected successor nodes. Naturally, such reports require the selection of an element before running the analysis. Reports can be printed or saved as a PDF file by using the corresponding buttons on the bottom of each report dialog. A report can be longer than its dialog window, which will result in a scroll bar on the right side of the window. Likewise, summary tables may obtain their own scroll bars.

5.1 Information System Summary

This is a straight-forward static report about the entire health information system. The `Summary Table` lists the `Total` number of nodes and edges by type. Further, it includes for each type the most important attributes and their occurrence. For attributes with a 1:1 cardinality, the percentage column (`%`) refers to the occurrence and the total adds up to 100 percent. For attributes with a 1:n cardinality, the same column generally can add up to more than 100 percent since multiple attributes can appear per node or edge. Average (`Avg`) refers to the average occurrence of the specific attribute per node or edge. Minimum (`Min`) and maximum (`Max`) indicates the respective number of minimal or maximal occurrence on one node for the specific attribute.

The `Node Type Pie Diagram` and `Edge Type Pie Diagram` illustrate the proportion of the respective type toward the total of elements. The `Node Owner Bar Diagram` lists all owners and the length of the bar indicates the number of nodes subject to each owner's responsibility. The stacked colors correspond with the colors of each node type in the `Node Type Pie Diagram`. Additionally, two lines are superimposed and are the sum of `incoming` and `outgoing` connections of each owner's nodes. `Outgoing` connections are an indicator of node importance for feeding other elements with data, whereas `incoming` connections are associated with data consuming nodes.



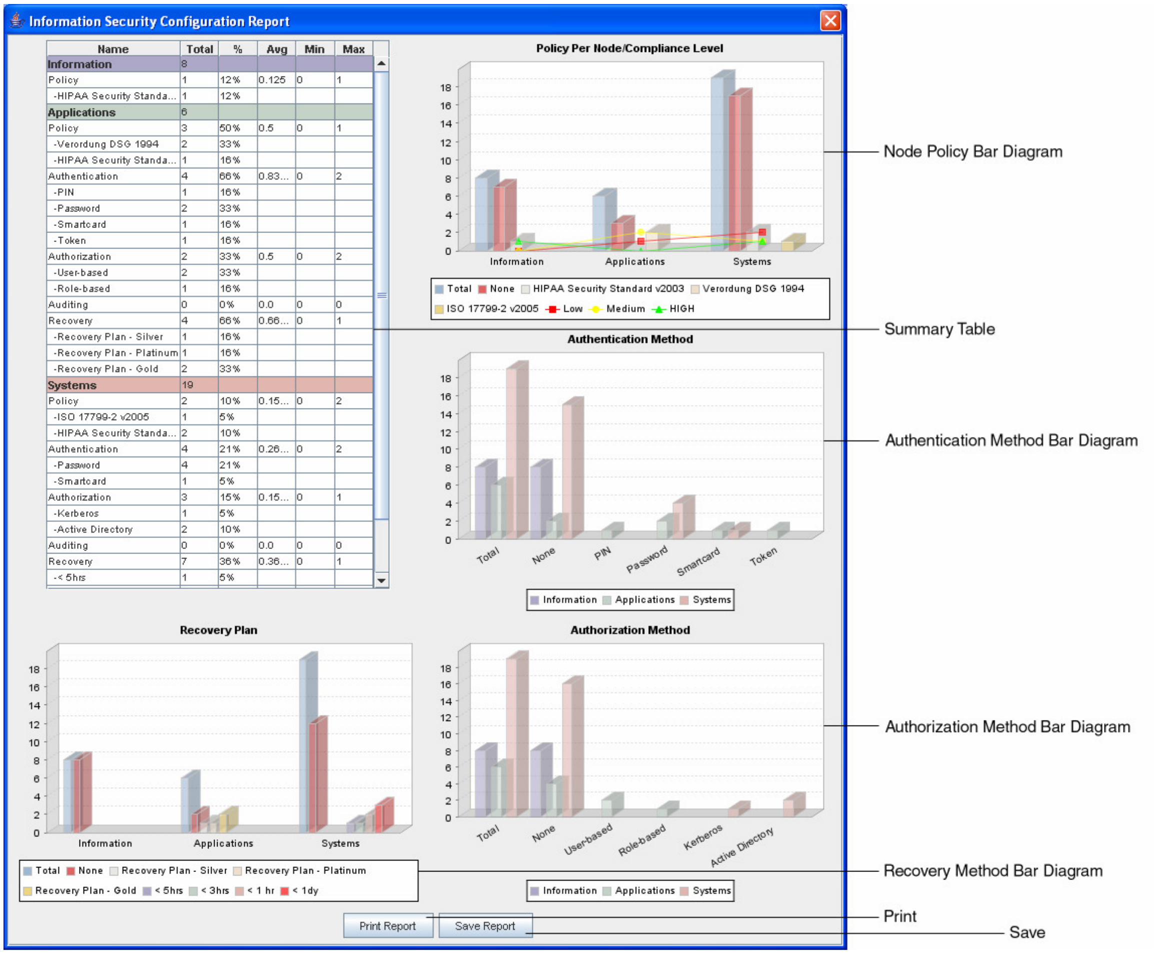
Information System Summary Report

Name	Total	%	Avg	Min	Max
Information	8				
Unit	0	0%	0.0	0	0
Function	0	0%	0.0	0	0
Data	0	0%	0.0	0	0
Applications	6				
Role	0	0%	0.0	0	0
Vendor	3		0.5	0	1
Data	0	0%	0.0	0	0
Systems	19				
Location	6		0.63...	0	1
-Campus - Registration	1	5%			
-Campus - Radiology	3	15%			
-Campus - Emergency	5	26%			
-Data Center 1	1	5%			
-Data Center 2	1	5%			
-Campus - Administration	1	5%			
Vendor	4		0.57...	0	1
-Sun	1	5%			
-HP	3	15%			
-IBM	4	21%			
-Dell	3	15%			
Os	6		0.63...	0	1
-Solaris	1	5%			
-Windows 2000	2	10%			
-Windows 2003	1	5%			
-Windows XP	5	26%			
-HP-UNIX	1	5%			
-Windows 98	2	10%			
Net	1		0.05...	0	1
-	1	5%			
Information Flow	6				
Application Flow	5				
Protocol	3		0.6	0	1

Figure 16: Information System Summary Report.

5.2 Information Security Configuration

The information security configuration report is structured in a similar way like the report discussed above. However, it is focusing on providing a summary of the security relevant properties of all the nodes and edges. Its Summary Table on the left is similarly organized and provides numbers organized by node types. The Node Policy Bar Diagram features grouped bars for all three node types. The first bar in each group provides the number of the total nodes of the specific type in the system. The second bar indicates the number of nodes that do not have security policies assigned at all. The subsequent bars signify used security policies and number their occurrence. The Y-Axis specifies the number of nodes. Superimposed are three lines that indicate the compliance status of the nodes. The color codes correspond to the ones of the policy indicator status described in 4.1.3. The Recovery Method Bar Diagram is organized in a similar fashion, the bars are grouped by node type, the first and second bar provide the total numbers and nodes without any assigned recovery method, followed by the assigned recovery methods or plans.



Name	Total	%	Avg	Min	Max
Information	8				
Policy	1	12%	0.125	0	1
-HIPAA Security Standa...	1	12%			
Applications	6				
Policy	3	50%	0.5	0	1
-Verordung DSG 1994	2	33%			
-HIPAA Security Standa...	1	16%			
Authentication	4	66%	0.83...	0	2
-PIN	1	16%			
-Password	2	33%			
-Smartcard	1	16%			
-Token	1	16%			
Authorization	2	33%	0.5	0	2
-User-based	2	33%			
-Role-based	1	16%			
Auditing	0	0%	0.0	0	0
Recovery	4	66%	0.66...	0	1
-Recovery Plan - Silver	1	16%			
-Recovery Plan - Platinum	1	16%			
-Recovery Plan - Gold	2	33%			
Systems	19				
Policy	2	10%	0.15...	0	2
-ISO 17799-2 v2005	1	5%			
-HIPAA Security Standa...	2	10%			
Authentication	4	21%	0.26...	0	2
-Password	4	21%			
-Smartcard	1	5%			
Authorization	3	15%	0.15...	0	1
-Kerberos	1	5%			
-Active Directory	2	10%			
Auditing	0	0%	0.0	0	0
Recovery	7	36%	0.36...	0	1
-< 5hrs	1	5%			

Figure 17: Information Security Configuration Report.

The Authentication Method Bar Diagram and Authorization Method Bar Diagram are grouped by attribute. The bar color for information, application, and system elements correspond to the colors found in the Summary Table. The first group includes bars for the total of all three node types. Accordingly the second group has bars for all types with no such methods assigned. Each attribute value has its own group with three bars for each node type.

5.3 Sub-Graph Compliance Report

This report type requires one specific node to be selected. Unlike the static reports described above, it calculates values that incorporate the property of the graph, specifically the weight of its edges, the nodes' degree, and distance from the root node. The following figure illustrates a simple graph, which shows the weight for each edge and the in- and out-degree for each node separated by a forward-slash. For example, the server node on the left has an in-degree of 1 (it has 1 incoming edge from the information node above) and an out-degree of 4 (3 outgoing connections to client nodes and one outgoing connection to the server node on the right). Therefore, all its outgoing edges obtain a weight of 0.25 (1 divided by the out-degree of the parent node).

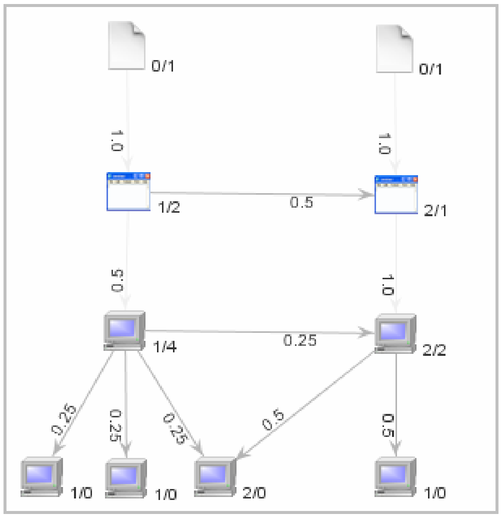


Figure 18: Graph properties.

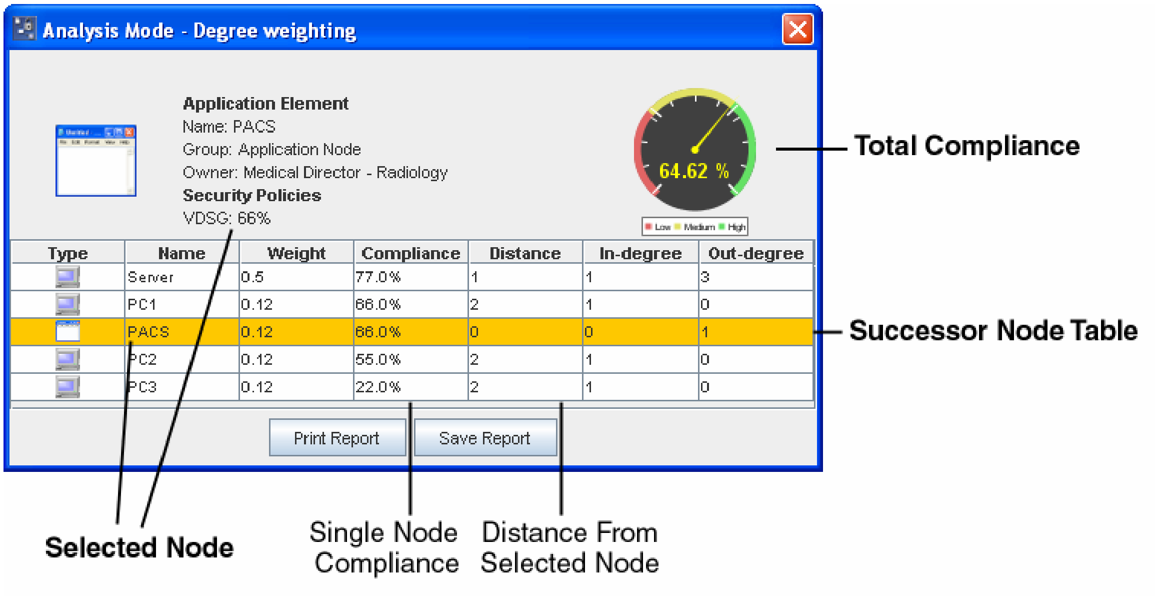
The analysis algorithm generally performs two steps: First, the compliance factor for each node is calculated independently of its neighbor nodes. Currently, it is derived from the total of compliant control items compared against the total of applied controls. However, this value could be obtained differently such as involving attribute values. Second, the weight of each node in the selected sub-graph is calculated depending on the chosen analysis mode and multiplied with the compliance factor. The sum of all these values result in the total compliance factor for the selected node.

Analysis Mode	
`Lowest Value`	The selected node obtains the lowest compliance value of all its successor nodes in the sub-graph. Naturally this mode provides a very low compliance value, which can be labeled as pessimistic.
`Evenly weighted`	Each node receives the same weight, independently of its position in the sub-graph.
`Degree weighting`	The node weights are calculated by normalizing their degrees. The more connected a node is, the higher its weight.

Distance weighting	The weight of a node decreases by its distance from the selected root node.
Recursive weighting	The weight of a node decreases by its distance from the selected node but is determined recursively, starting with the child nodes first. This is an experimental mode, since the nodes values are calculated recursively no node weights are currently provided.

Table 5-1: Analysis modes.

In the recursive analysis mode, a function call recursively traverses the graph originating from the selected node down until it reaches a node without further successor nodes. It then starts calculating and aggregating the compliance values, weighted by the degree of the nodes (cf. Figure 18). The aggregated value of a parent node is calculated by its own single node compliance and the single node compliance of all its children. Both values are weighted with a factor of 0.5. This analysis mode is experimental and generally provides results, which are too optimistic.



Application Element
Name: PACS
Group: Application Node
Owner: Medical Director - Radiology
Security Policies
VDSG: 66%

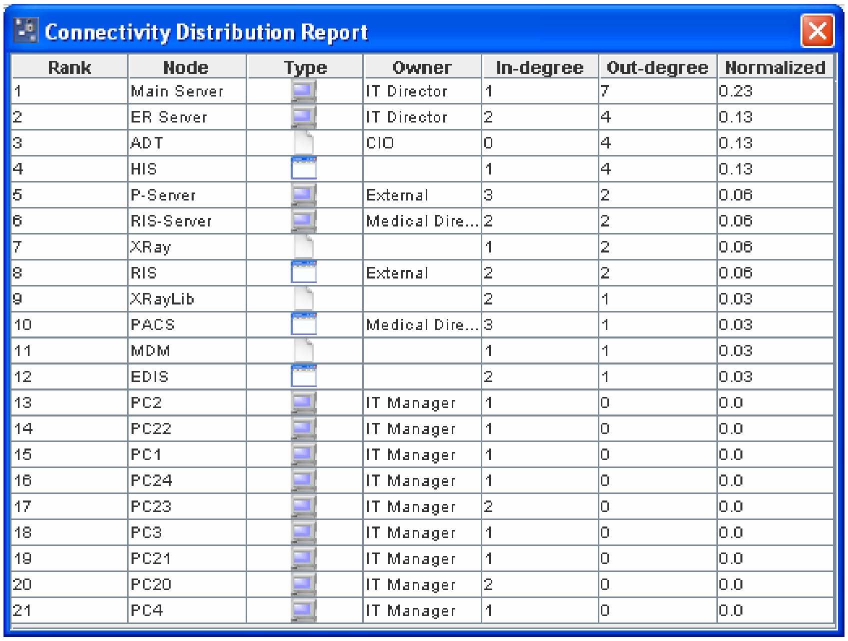
Type	Name	Weight	Compliance	Distance	In-degree	Out-degree
🖥	Server	0.5	77.0%	1	1	3
🖥	PC1	0.12	66.0%	2	1	0
□	PACS	0.12	66.0%	0	0	1
🖥	PC2	0.12	55.0%	2	1	0
🖥	PC3	0.12	22.0%	2	1	0

Table 5-2: Node compliance report.

The results of all analysis modes are presented in the form of a table. The root node of the sub-graph is highlighted in the table and naturally has a distance from the selected node of zero. The table is ordered by single node compliance. Further a speedometer-like figure indicates the calculated total compliance for the selected node.

5.4 Connectivity Distribution Report

This report presents a list of all nodes ranked by their degrees. It is assumed that nodes with many outgoing connections are more important in a graph than nodes with few connections. Therefore, information security activities should focus in particular on nodes with many outgoing connections since their importance is high and their failure has the most consequences for the entire system.



Rank	Node	Type	Owner	In-degree	Out-degree	Normalized
1	Main Server	🖥	IT Director	1	7	0.23
2	ER Server	🖥	IT Director	2	4	0.13
3	ADT	📄	CIO	0	4	0.13
4	HIS	🗔		1	4	0.13
5	P-Server	🖥	External	3	2	0.06
6	RIS-Server	🖥	Medical Dire...	2	2	0.06
7	XRay	📄		1	2	0.06
8	RIS	🗔	External	2	2	0.06
9	XRayLib	📄		2	1	0.03
10	PACS	🗔	Medical Dire...	3	1	0.03
11	MDM	📄		1	1	0.03
12	EDIS	🗔		2	1	0.03
13	PC2	🖥	IT Manager	1	0	0.0
14	PC22	🖥	IT Manager	1	0	0.0
15	PC1	🖥	IT Manager	1	0	0.0
16	PC24	🖥	IT Manager	1	0	0.0
17	PC23	🖥	IT Manager	2	0	0.0
18	PC3	🖥	IT Manager	1	0	0.0
19	PC21	🖥	IT Manager	1	0	0.0
20	PC20	🖥	IT Manager	2	0	0.0
21	PC4	🖥	IT Manager	1	0	0.0

Figure 19: Connectivity distribution report.

6 Known Issues

- Changing the application window size can occasionally offset the model with the background line when zooming and panning. Pressing the resize button readjusts the model to the new application window size.
- Zooming and panning positions are not stored in the model and have to be adjusted each time a model is loaded.
- Printing reports does not adjust the graphics to the correct paper size.
- Saving reports currently does not work.
- Constraints of the graph during modeling are not enforced.

7 Planned Features

- Security reports, which are based on function, unit, data, etc.
- Security reports, which consider attribute values to calculate node compliance.
- Editors for policies and option lists.
- Refined policies whose controls only apply to specific node types.
- Risk catalog, items assignable to nodes including probabilities.
- Interfaces to other production applications to import external data.
- Group modeling capabilities for similar objects (such as PCs).

External Libraries Used

Name	Version	URL
Apache Jakarta Commons Collections	3.1	http://jakarta.apache.org/commons/collections
Apache Jakarta Commons Logging	1.0.4	http://jakarta.apache.org/commons/logging/
Apache XML Commons	1.0	http://xml.apache.org/commons
Castor XML	0.9.9.1	http://www.castor.org
Cern Colt Scientific Library	1.2.0	http://dsd.lbl.gov/~hoschek/colt
iText	1.4	http://www.lowagie.com/iText/
Java Universal Network/Graph Framework (JUNG)	1.7.4	http://jung.sourceforge.net
JCommon	1.0.2	http://www.jfree.org/jcommon
JFreeChart	1.0.1	http://www.jfree.org/jfreechart/
Xerces2 Java Parser	2.8.0	http://xml.apache.org/xerces2-j/index.html