

MANUAL

Version 3.0.1



 **RM Studio**

Does your company stand out of the crowd?



Certificate No. IS 67387
ISO 27001



Certificate No. FS 67386
ISO 9001

INTRODUCTION

INTRODUCTION

The RM Studio® application is intended for use by companies, institutions and government entities that wish to guarantee security in the processing of information. The program is based on the methodology of the ISO/IEC 27001:2005 and ISO/IEC 27002:2005 security Standards. In this document the Standards will be referred to as ISO/IEC 27001 and ISO/IEC 27002, respectively. RM Studio® is a Microsoft-compatible software that is developed in Microsoft Visual Studio. Software development is done in accordance with procedures from Microsoft Solution Framework and certified by the British Standards Institution in accordance with ISO 9001 and ISO/IEC 27001.

ABOUT THIS MANUAL

This is the User Manual for the RM Studio® application, version 3. The application maintains an overview of, and manages risks in the operation of companies and organizations. RM Studio® is an application designed to assist the user in the preparation of Risk Assessments as well as Risk Management. Multiple Business Entities and Risk Assessments can be registered in the system.

WHAT IS RISK MANAGEMENT

Risk Management is the act of using Standards to reduce risk. The ISO/IEC 27001 security Standard provides businesses with a clear way to mitigate risks in information security. ISO 14001 helps companies to manage environmental risks while ISO 9001 deals with quality issues.

RM Studio® has Standards embedded in the software. RM Studio® is based on the methodologies of the ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005 security Standards and the software guides users through the process of Risk Assessment, Gap Analysis and Risk Treatment.

WHAT WILL RM STUDIO DO FOR YOUR COMPANY

RM Studio® will help your organization clarify its vision in regards to Risk Management. RM Studio® will guide you through these processes and bring traceable manageability without the tedium. RM Studio® will also ensure that your risk assessments are comparable and reproducible.

RM Studio® divides Risk Management into 3 processes: *Risk Assessments, GAP Analysis and Risk Treatment.*

RISK ASSESSMENTS

In regards to a particular Standard, with what is needed to be eligible for certification.

RM Studio® will assist you in evaluating the implementation status of each Control on a global level. This is necessary for obtaining certification according to international Standards. Going through the Controls for the Standard you are able to evaluate the applicability of each Control in regards to your company and give your justification for your choices. This will streamline the evaluation process and ensure traceability.

GAP ANALYSIS (OPTIONAL PROCEDURE)

RM Studio® will qualitatively evaluate the Current Information Security Risk and Future Information Security Risk of your organization or given Business Entity from the data available. Current and Future Information Security Risk is calculated with regards to the status of the Controls of a given Standard. The software will assist you in reacting to positive and negative developments in Risk. You will also be able to secure your information according to ISO Standards.

RISK TREATMENT

Through the use of RM Studio® you will streamline Risk Management and reduce complexity and cost. This will be a major asset in obtaining a certification of compliance to international Standards.

Through the reporting capabilities of RM Studio® you can produce reports that you can use to keep track of the status of your certification as well as inform others.

CONTACT AND FEEDBACK

Please send any suggestions or comments regarding this manual or the software to Stiki by sending an email to support@stiki.eu, or by phoning +354 5 700 600.

Any input will be recorded, viewed and used in future revisions of the software.

TABLE OF CONTENTS

INTRODUCTION	2	RESET STANDARD DATA	23
ABOUT THIS MANUAL	2	STANDARD CONTROLS	24
WHAT IS RISK MANAGEMENT	2	WORKING WITH THE CONTROLS	24
WHAT WILL RM STUDIO DO FOR YOUR COMPANY	2	CREATING NEW STANDARDS AND CONTROLS	24
RISK ASSESSMENTS	3	9. REPORTS	25
GAP ANALYSIS (OPTIONAL PROCEDURE)	3	THE STANDARD REPORTS:	25
RISK TREATMENT	3		
CONTACT AND FEEDBACK 3		NEW REPORTS	26
TABLE OF CONTENTS	4	10. RISK ASSESSMENTS	27
1. GETTING STARTED	5	WORKING WITH ASSESSMENTS	27
REQUIREMENTS	5	CREATING AN ASSESSMENT	27
SHORTCUTS	5	COPY RISK ASSESSMENT	27
EXPIRATION	5	SCOPE AND BASIC CRITERIA	27
LICENSING	6	EXAMPLE OF BASIC CRITERIA	28
2. NAVIGATION	7	WORKING WITH ASSETS	28
SECURITY	7	ASSETS RETRIEVED	28
ROLES	7	OWNER	28
TASKS	7	OPERATOR	29
USERS	7	EVALUATION VALUES	29
PROPERTIES	8	CONFIDENTIALITY	29
DATABASE	8	INTEGRITY	29
ADD A DATABASE SERVER	8	AVAILABILITY	29
UPGRADE DATABASE	9	VALUE	29
CREATE NEW DATABASE	9	DEFINITIONS OF VALUE AND PROPERTIES	29
DEPLOY DATABASE	9	RISKS	30
STANDARD DATA	9	ADDING RISKS	30
DEPLOY STANDARD	9	AGGREGATED VIEW OF RISKS	30
DEFAULT DATA	10	RELATIONSHIP BETWEEN ASSETS AND THREATS	30
REPORTING	10	PROPERTIES	30
AUTHORIZATION STORE	10	IMPACT OF THREAT	30
EVALUATION TEMPLATES	11	PROBABILITY OF THREAT	30
SHORTCOMINGS OF EVALUATION TEMPLATES	11	VULNERABILITY OF ASSET	30
CATEGORIES	11	HISTORY	31
LANGUAGES	12	ITEM HISTORY	31
ABOUT	12	VIEW ITEM	31
REGISTRATION	12	CHANGES SET DETAILS	31
HELP	12	VIEW RISK ASSESSMENT VERSION	32
APPLICATION STYLIST	12	11. GAP ANALYSIS	33
NAVIGATING RM STUDIO	13	CREATING A NEW GAP ANALYSIS	33
NAVIGATION TREE	13	GAP ANALYSIS INFORMATION	33
TABS	13	CONTROLS	33
3. FEATURE USAGE	14	IMPLEMENTATION	33
SAVE FUNCTION	14	STATUS	34
THE GRID	14	JUSTIFICATION	34
CLEAR USER CACHE	14	12. RISK TREATMENT	35
GROUPING BY COLUMN	14	WORKING WITH RISK TREATMENT	35
GROUPING BY SUBCATEGORIES	15	RISK CRITERIA	35
POWERFUL SEARCH	15	ASSET LEVEL	36
EXPORT FACILITIES	15	CONTROLS TAB	36
4. INTRODUCTION	16	SCHEDULING A FUTURE CONTROL	37
ENTITIES	16	FUTURE CONTROLS TAB	37
BUSINESS ENTITIES	16	OVERVIEW	37
ASSETS	16	RELOAD ASSETS, THREATS AND CONTROLS	37
THREATS	16	13. DEFINITIONS	39
STANDARDS	16	DEFINITION OF ASSET EVALUATION VALUES	39
PROCESSES	17	DEFINITION OF THREAT EVALUATION VALUES	40
RISK ASSESSMENT	17	IMPACT OF THREAT	40
GAP ANALYSIS	17	14. GLOSSARY	41
RISK TREATMENT	17	15. CONTEXT & FLOW	44
WORKING WITH THE PROCESSES	17	CONTEXT	44
REPORTING	18	FLOW	45
REPORTS	18	16. CALCULATIONS	46
5. BUSINESS ENTITIES	19	SECURITY RISK	46
STARTING TO USE		1.	46
RM STUDIO®	19	2.	46
CREATING A NEW BUSINESS ENTITY	19	3.	46
6. ASSETS	20	4.	47
WHAT ARE ASSETS	20	RESIDUAL RISK	47
DEFINING ASSETS	20	17. CREDITS	48
CREATING A NEW ASSET	20	ICONS IN RM STUDIO	48
DESCRIPTION	20	FRONT PAGE	48
CATEGORIES	20	COPYRIGHT	48
7. THREATS	22		
CREATING A NEW THREAT	22		
CATEGORIES	22		
THREATENED ASSETS	22		
MITIGATING CONTROLS	22		
8. STANDARDS	23		
AVAILABLE STANDARDS	23		
HOW TO INSTALL A STANDARD	23		

I. GETTING STARTED

REQUIREMENTS

The software and hardware requirements necessary for installing and running RM Studio® version 3.0 are as follows:

Minimum system requirements for XP Pro:

Processor: Intel 1.5 GHz or similar

Memory: 512 MB

Operating System: Windows XP Pro with service pack 3 and above

Disk space: 2 GB free disk space

Display: 1024x768

For local database: SQL Express 2005 Advanced with or 2008

Minimum system requirements for Vista and Windows 7:

Processor: Intel 1.8 GHz or similar

Memory: 1024 MB

Disk space: 2 GB free disk space

Display: 1024x768

For local database: SQL Express 2005 Advanced with SP3 or 2008

Recommended system requirements for XP Pro:

Processor: Intel 2.4 GHz or similar

Memory: 2 GB

Operating System: Windows XP Pro with service pack 3 and above

Disk space: 2 GB free disk space

Display: 22", 1680x1050

For local database: SQL Express 2005 Advanced with SP3 or 2008

Recommended system requirements for Vista and Windows 7:

Processor: Intel 2.4 GHz or similar

Memory: 2 GB

Disk space: 2 GB free disk space

Display: 22", 1680X1050

For local database: SQL Express 2005 Advanced or 2008

For further information on Server Requirements see also:

[http://technet.microsoft.com/en-us/library/ms143506\(SQL.100\).aspx#Express32](http://technet.microsoft.com/en-us/library/ms143506(SQL.100).aspx#Express32)

and

<https://www.microsoft.com/sqlserver/2005/en/us/system-requirements.aspx#32>

SHORTCUTS

During the installation of RM Studio®, shortcuts are created on the desktop and in the Start menu under the path Start > All programs > Stiki > RM Studio.

EXPIRATION

When the license is about to expire the system will remind you by showing how many days are left on the license (image 1.1).

For license information, contact Stiki ehf. by sending an email to support@stiki.eu or phoning +354 5 700 600.

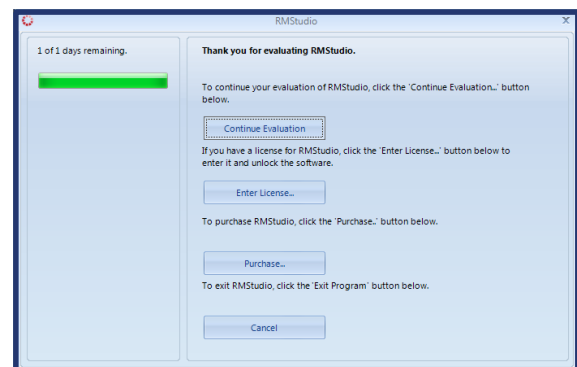


Image 1.1 - Expiration Notice

By default there is only one account in RM Studio®, the Administrator account. The Administrator account uses the username: "Administrator" and the password "Administrator". The first thing you should do after you log in is to connect to a

database and change the password for the Administrator account. To change a Users password navigate to the Users tab in the Security dialog (image 1.2).

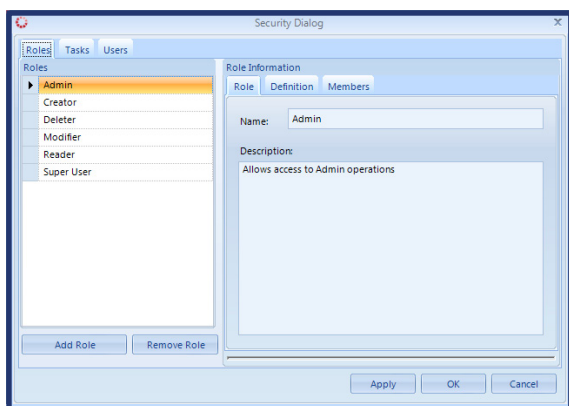


Image 1.2 - RM Studio Security Dialog

There select the appropriate User and click on the Change Password button. The window in image 1.3 should pop up. You can only change the password for RM Studio Users not Windows Users.

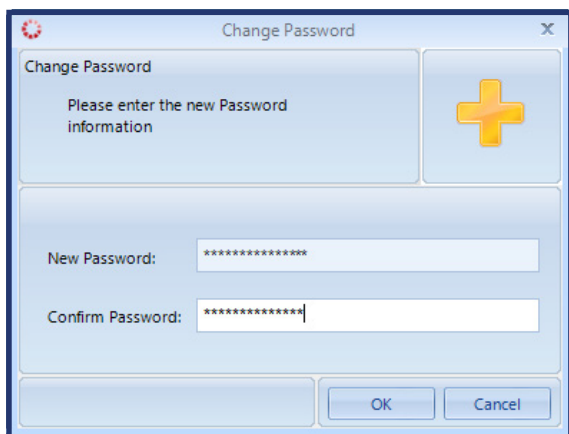


Image 1.3 - Change Password Dialog

Remember that the usernames and passwords are case sensitive. Users can either be Active Directory Users (Windows Users) or defined in RM Studio®, as local RM Studio users which are defined and used only within the application.

When logging in you will see a drop down box which gives you the choice between the two (image 1.4). When logging in as a Windows User in you can choose to use the Current Domain by checking the “Use Current Domain” box (image 1.4).

How to add new users will be covered in the next chapter.

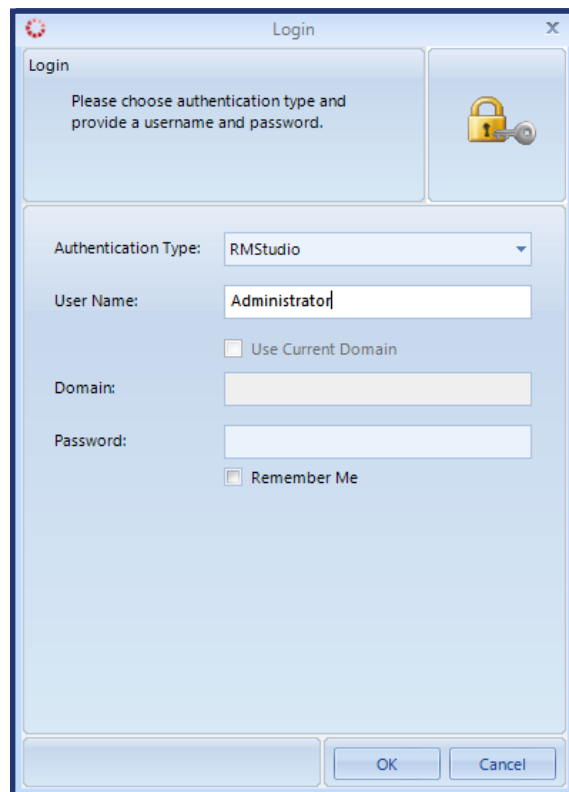


Image 1.4 - RM Studio Login Window

LICENSING

To add a new license to RM Studio® you must click on the Registration button (image 1.5) on the Menu Bar. We will go into details about licensing in chapter 2.

For license information, contact Stiki ehf. by e-mailing RMSsupport@stiki.eu or phoning +354 5 700 600

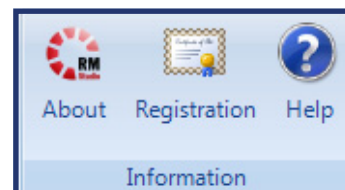


Image 1.5- RM Studio Menu Bar

2. NAVIGATION

RM Studio's Menu Bar (image 2.1) has been conformed to the Office 2007 look and feel. This is one of many improvements to make RM Studio® easier to use and more efficient. There are two tabs on the Menu Bar, Home and Styles.

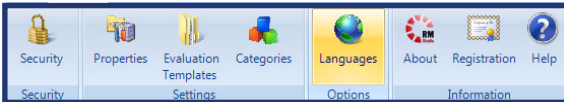


Image 2.1 - Menu Bar

SECURITY

The security features in RM Studio® make it possible to define exactly the roles of different user groups.

The basic element used to construct a Role are the Operations. RM Studio® has different operations that together define everything that can be done in RM Studio®. These operations can be further grouped into Tasks. Roles can then be defined to include certain Operations or Tasks.

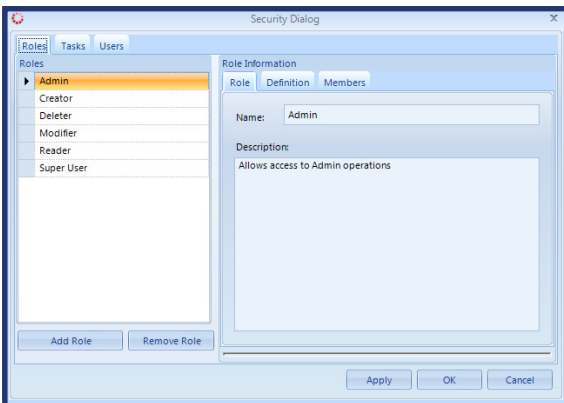


Image 2.2 - Security Dialog

ROLES

RM Studio comes with a predefined set of 6 Roles. If you need to add a new Role click on the Add Role button (image 2.3) and the dialog box in image 2.4 will appear. When you have filled out the necessary information click OK.

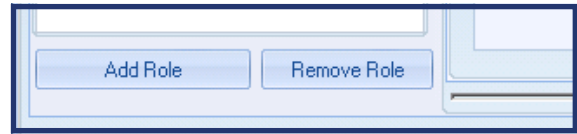


Image 2.3 - Add Role Button

After you have created a Role you can then define it under the Definition tab (image 2.2). By clicking the “Add” button you can add Operations, Tasks, or sub Roles to the new Role as appropriate.

The third tab is the “Members” tab. Here you can assign different users to the Role. Likewise, under the “Users” tab you can assign Roles to individual users.

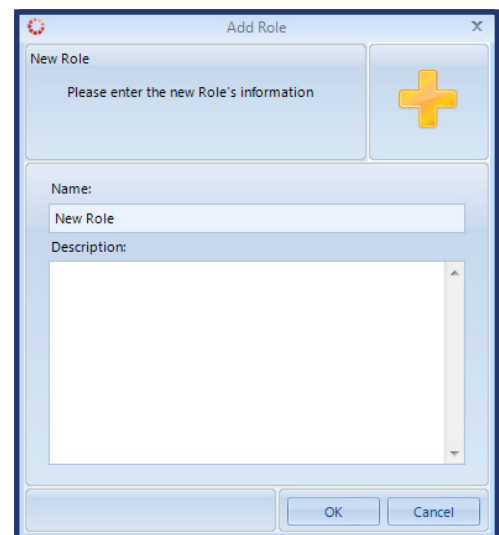


Image 2.4 - Add Role

TASKS

Tasks define what a particular role can do in RM Studio®. Adding a new Task is similar to adding a new Role; you need to navigate to the Tasks Panel and click the “Add Task” button. One Task is made up from many Operations. Adding Operations to a Task is just like adding Tasks, Operations and sub Roles to a Role. You can even add other sub Tasks to a Task just like you could with Roles.

USERS

The Users of RM Studio® can be either Integrated Windows users (Active

Directory) or locally defined RM Studio Users.

To add a user navigate to the User Tab and click on the “Add User” button. The window in image 2.5 should appear. If you select Integrated Windows user you will have to fill in the “Windows login” and “Password”. In RM Studio® you can also add a Domain of your choice.

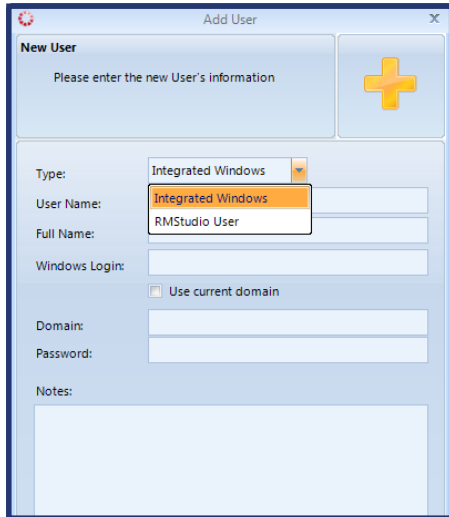


Image 2.5 - Add User

If you choose RM Studio User you will have to make a new password and confirm it (image 2.6).

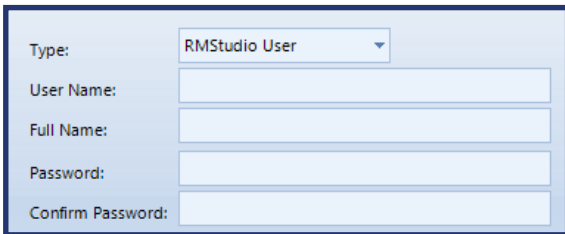


Image 2.6 - Adding RM Studio User

PROPERTIES

The second item on the Menu Bar is Properties (image 2.1). The Properties window is divided into four areas, Database, Reporting and Authorization Store.

DATABASE

Under Database you can configure which Server RM Studio® uses. By default the application will have no Servers defined (image 2.8).

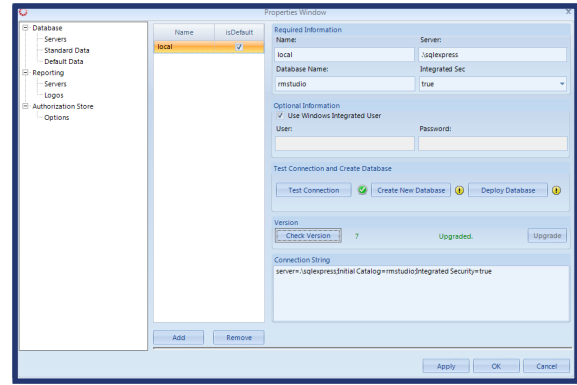


Image 2.7 - Properties Window

ADD A DATABASE SERVER

To add a database server click on the “Add” button below the list of Servers. A “New Database Server” window will appear (image 2.8). In this window you will have to fill in the Name, Server, Database Name, and Integrated Security fields. The Name field is a name that you give the Database instance, Server is the name of the server where the Database resides on your network, Database Name is the name of the RM Studio® database on your server and Integrated Security dictates whether or not IWA (Integrated Windows Authentication) is used on the Server.

When you have entered the necessary information and clicked OK you can test the connection by clicking on the “Test Connection” button. If the icon turns green then a connection with the server was established. If the icon turns red the connection failed.

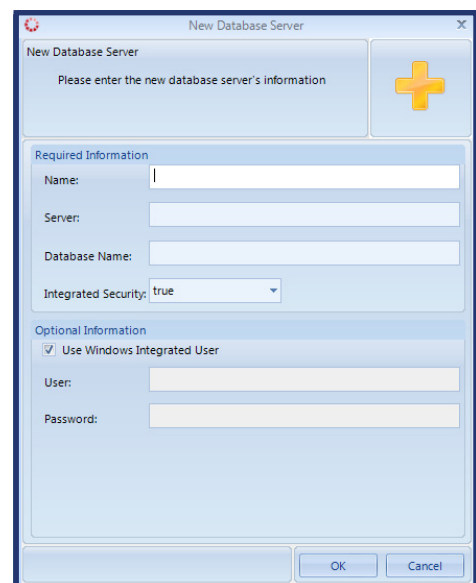


Image 2.8 - New Database Server

UPGRADE DATABASE

If you have a previously installed RM Studio database and would like to continue using it, you can upgrade it to the latest version. Before continuing we strongly suggest you back up your Database.

Start up RM Studio and open the Properties dialog. Make sure that you have a connection string to the database you wish to upgrade. If it is not there, enter it and mark it as default. Click Test Connection if you wish to verify that it is correct. If the string was already correct and marked as default you can continue directly with the upgrade. If not, you must restart RM Studio.

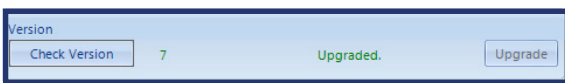


Image 2.9 - Upgrade Database

Click on the Check Version button, it should tell you the version number and if your database is out of date. If your Database is **out of date** the upgrade button should become enabled.

Note that there are several large, atomic actions taken, so the progress bar may seem to stand still for a while. Please wait patiently and allow the upgrade to complete. If for any reason the upgrade fails, restore your database and restart the upgrade.

Once it completes, the properties window should tell you that your database version is upgraded and RM Studio is now ready for use.

CREATE NEW DATABASE

The Create New Database button (image 2.9) allows you to create a New RM Studio database on the Database Server that you are connected to from within RM Studio®.

To create a new RM Studio® database make sure that you name the connection in a descriptive manner, that you have the name of the server, the name of the Database and the type of security settings that apply to your network. Click “OK” and then “Test Connection” button (image 2.9). Creating a new database will take a few moments.

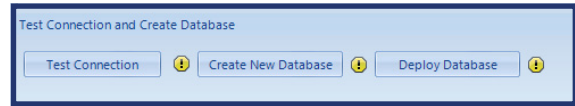


Image 2.9 - Create New Database

DEPLOY DATABASE

When a Database has been imported you need to Deploy the Database. That is done by selecting the newly created Database and then you press Deploy Database (image 2.9b). When you Deploy you are actually adding the schema to the Database. This process is only needed when you add an older Database to RM Studio. When you create new Databases they get Deployed automatically.

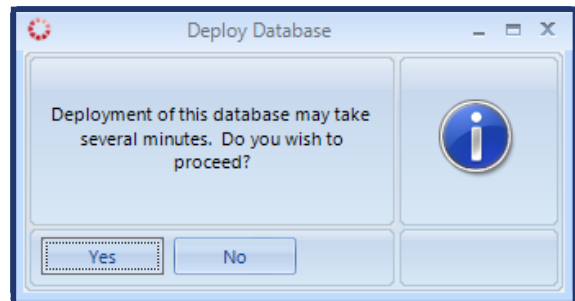


Image 2.9b - Deploy Database

STANDARD DATA

This is a new feature in RM Studio®. Here you can see all the Standards you can deploy into your RM Studio®. You can also reset the Standards you have altered.

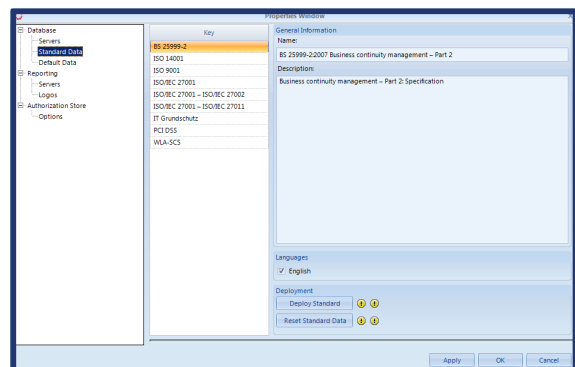


Image 2.9c - Standard Data

DEPLOY STANDARD

To deploy a Standard into RM Studio®, you will have to have bought the Standard from Stiki and have the right key registered in the registration window (image 2.19). If all these steps have been completed the

Standard Data window should show the Standards available to you. Further detail on installation of Standards will be covered in chapter “8. STANDARDS” on page 24.

DEFAULT DATA

Is where Administrators can reset all predefined data to their original state.

The options are, All Default Data, Threats only, Categories only, Evaluation Templates or Threat Categories (image 2.9d).

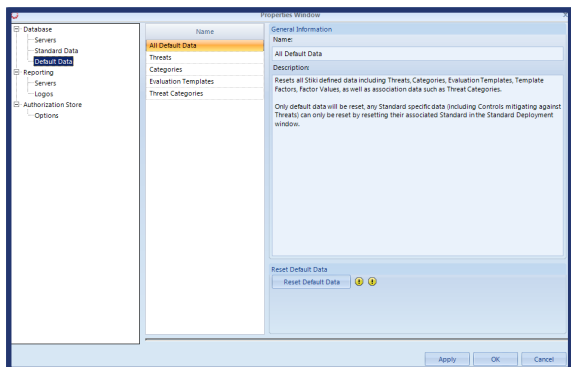


Image 2.9d - Reset to Default Data

When you have selected the option you would like to reset press the Reset Default Data button. When pressed all changes made to the selected data will be reverted to its original state. This will not affect data entered into the Processes and Entities.

REPORTING

There are two options under Reporting “Servers” and “Logos”.

Under Servers (image 2.10) you can configure where the Reporting Server and the Reporting Service reside as well as the Reporting Path. In RM Studio® we also have Local Reports Module. When using the Local Reports Module the Reporting Server is incorporated into RM Studio and there is no network configuration needed to run the reporting services and reports can be generated with ease on the fly.

In the case of shared customized reports we recommend using Server Reports. We have an installation manual for those who prefer to set up Reporting services. Please send an e-mail to our Customer Service asking for a copy of the Microsoft Reporting Services Installation Guide.

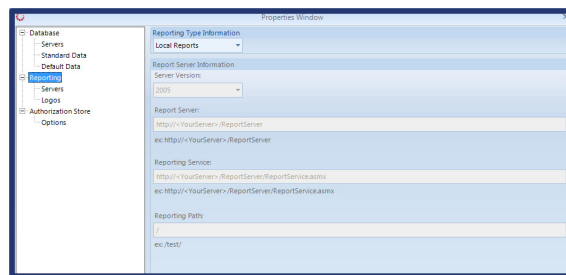


Image 2.10 - Reporting Servers

Under Logos (image 2.11) you will find a list of the logos you can use when generating Reports from RM Studio®. This list is empty by default.

When you add a logo to the RM Studio® application you will have to define them as “Large” or “Small”, this categorizes the logos so that they will appear in the respective lists when you generate reports. Large logos are used for the front page and Small logos are used for the header. Please note that the Reporting Server must have access to the location where the logos are stored.

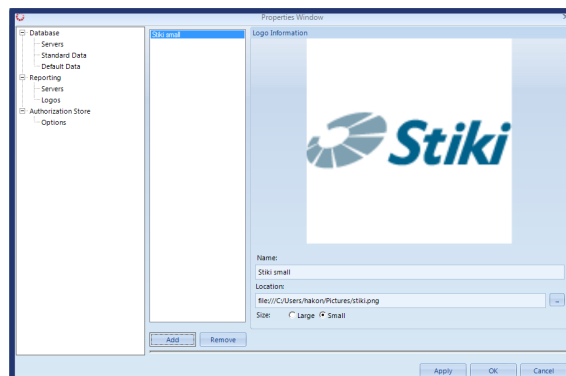


Image 2.11 - Reporting Logos

AUTHORIZATION STORE

The Authorization Store is where authorization information is kept in RM Studio®. Here the data defining Users, Roles, Tasks and Operations is stored.

In order for this information to be accessible centrally the Authorization Store must be stored in a central location, e.g. central server.

To do this copy the XML file from its default location (C:\Program Files\Stiki\RMStudio\RMStudioPolicyStore.xml) and paste it into a shared folder on your SERVER. Open the Properties window in RM Studio > Authorization Store > Options and point to the file in the shared folder on your SERVER.

(image 2.12).

This needs to be done for every machine that uses the centralized information.

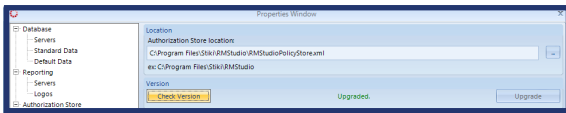


Image 2.12 - Properties Window

EVALUATION TEMPLATES

The next item on the Menu Bar is Evaluation Templates; these are used to qualitatively evaluate Threats and Assets in RM Studio®. Users can add their own Asset or Threat Evaluations or change the definition of the Standard Asset and Threat Evaluations.

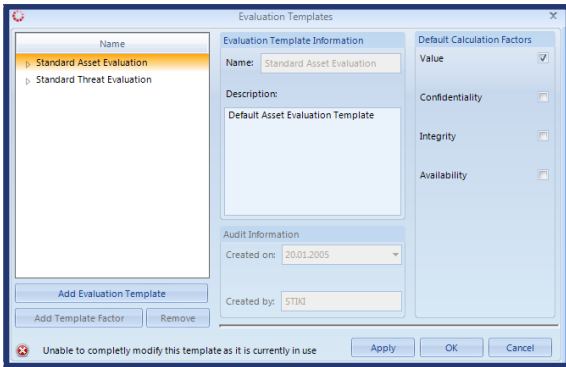


Image 2.13 - Evaluation Templates

To add a new Evaluation Template click the “Add Evaluation Template” button (image 2.13) and give the Evaluation Template a name. When you have a new Evaluation Template highlighted in the list on the left hand side you will be able to “Add Template Factor” by pushing the appropriate button (image 2.14). Every Evaluation Template can hold more than one Template Factor.

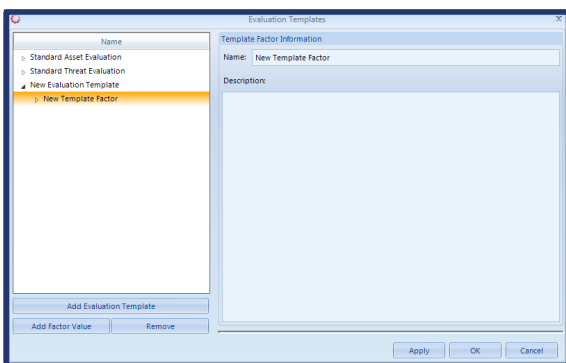


Image 2.14 - New Template Factor

When you have added a Template Factor

you can add a Factor Value. To do so you need to highlight the Template Factor that you wish to add a Factor Value to. The “Add Template Factor” button will change to an “Add Factor Value” button (image 2.15). Click on it to add a Factor Value.

When Asset Evaluation Templates are in use they can only be partially modified, such as changing the definitions of factor values as well as the defaults for security risk calculations.

SHORTCOMINGS OF EVALUATION TEMPLATES

- If an Evaluation Template has no Template Factor then it can not be used as either a Threat Template or as an Asset Template for a new Risk Assessment.
- If an Evaluation Template has any Factor Value equal to 0 (zero) then it can not be used as either a Threat or Asset Template for a new Risk Assessment.
- There may not be more than one Evaluation Template with the same name, names should be unique for each Template.
- There may not be more than one Template Factor in the same Evaluation Template with the same name. Names of Template Factors should be unique within a single Evaluation Template.
- There may not be more than one Factor Value in the same Template Factor with the same name. Names of Factor Values should be unique within a single Template Factor.
- Every change made to the Standard Templates will affect the calculations in the Processes using the default factors.
- The algorithm used for calculating security risk is most accurate when factor values start at value 1 (one) and the increment between values is 1 (one).

CATEGORIES

The next item on the Menu Bar is Categories.

Users of RM Studio® can define their own Categories for Assets or modified the system library. Categories can be defined as Parent or Sub Categories (image 2.16).

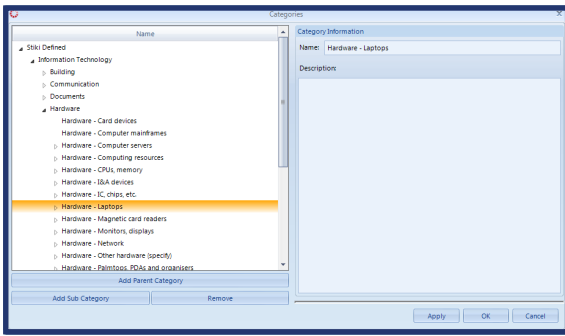


Image 2.16 - Categories

To add a new Parent Category click on the Add Parent Category button (image 2.17) and type in the Name and Description in the appropriate fields. To add a new Sub Category first select the appropriate Parent Category from the list and then click on the “Add Sub Category button”.

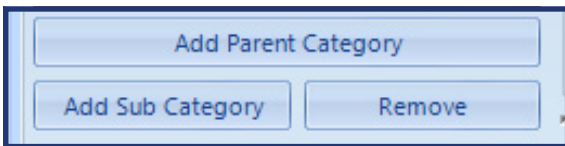


Image 2.17 - Drop Down List

LANGUAGES

The next item on the Menu Bar is Languages (image 2.1). RM Studio® currently supports English, German and Icelandic (image 2.18).

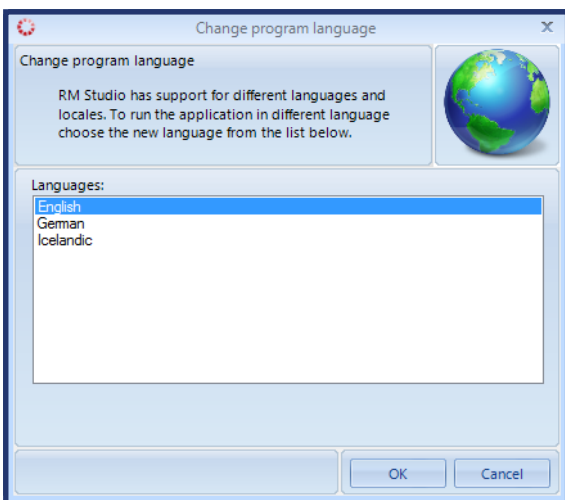


Image 2.18 - Languages

RM Studio® is shipped with English as the default language. If you wish to run RM Studio® in German or Icelandic please contact our sales representative in order

to obtain a license that will open up these options. Entering licenses will be covered in the “Registration” section of this chapter.

ABOUT

The next item on the Menu Bar is the About window. The About window displays information such as Version number and copyright notices.

REGISTRATION

Since version 2.1 RM Studio® has offered its users to pay for access to different data and functionality based upon their needs. In order to learn more about the price structure of the license system please contact our sales representatives.

To enter a new license click the Registration button on the Menu Bar. The Licenses window in image 2.19 will appear. Enter the Serial Number that you were provided into the text box and click on the “Apply License” button. All available features will then be displayed.

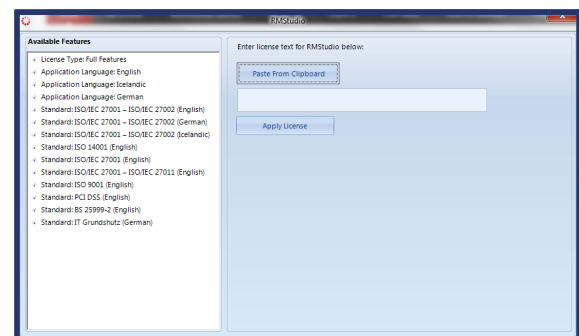


Image 2.19 - Registration

HELP

By pressing the “Help” button you will open up a PDF version of this Manual.

APPLICATION STYLIST

On the second tab of the Menu Bar you will find Styles. (Image 2.1). The Application Stylist is a powerful tool that allows the user to change just about anything regarding the look of RM Studio® (image 2.21). You can read more about the Application Stylist at the official online help page which can be found here: <http://help.infragistics.com/Help/NetAdvantage/NET/2008.3/CLR2.0/html/>

Win_Application_Styling.html.

Once you have created and saved a style it should appear in the drop down list on the styles tab (image 2.22).

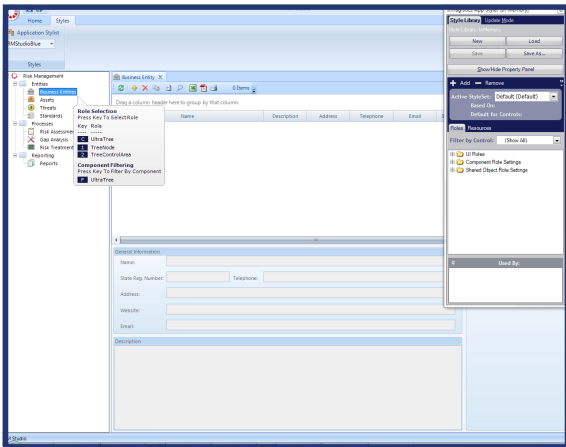


Image 2.21 - Application Stylist

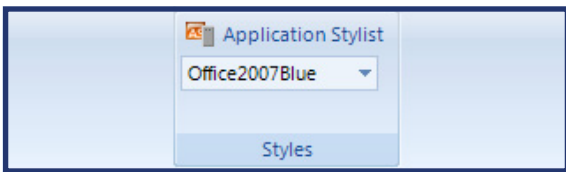


Image 2.22 - Application Stylist Drop Down

NAVIGATING RM STUDIO

NAVIGATION TREE

The Navigation Tree is on the left hand side of the RM Studio window (Image 2.23). The Navigation Tree groups the various functions into Processes, Entities and Reporting. From the Navigation tree you can access all these functions by double clicking on them.

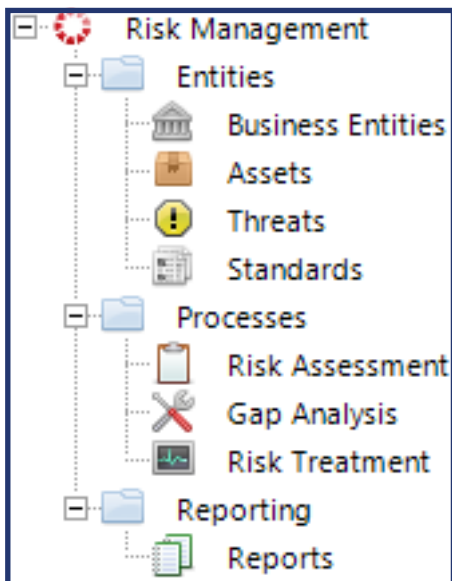


Image 2.23 - Navigation

RM Studio® utilizes tabs to provide the user with a clean and orderly working environment. New elements are opened up in a new tab (image 2.24) so the user can easily navigate between different items and functionality in RM Studio®.



Image 2.24 - Tabs in RM Studio

REVERT TO DEFAULT STYLE

If the GUI becomes illegible on account of the Application Stylist you can always revert to the RM Studio® default style, which is RM Studio Blue. Just select this style from the drop down list (image 2.22) and the GUI is reset.

3. FEATURE USAGE

SAVE FUNCTION

There are two save functions in RM Studio®. One is the Single Save Button (image 3.1), this button saves only the current tab you are working on. The other is the Cascading Save Button (image 3.2) or Save All button, this button saves all the information on all tabs that you are working on.



Image 3.1 - Single Save Button and Cascading Save Button

You will also find the save functions under the RM Studio® button (image 3.3). Under the RM Studio button you will also find the Clear User Cache function. See Clear User Cache under, The Grid paragraph.

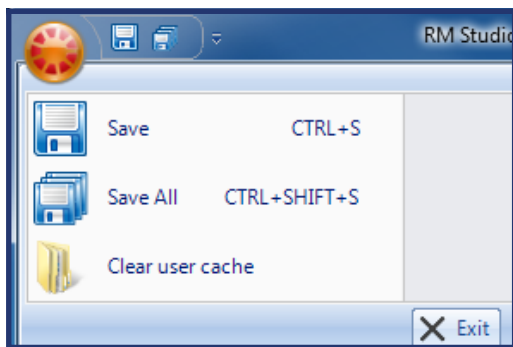


Image 3.3 - Stiki Button

Under the RM Studio button you will also find an Exit button to close the application.

If you right click on the tabs you will get a context menu with similar functionality where you can choose to save, save and close the tab, or simply close the tab (image 3.4).

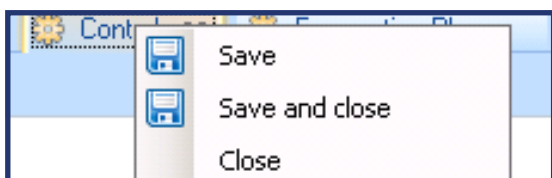


Image 3.4-Tab Commands

THE GRID

The RM Studio® Grid that is used to display most of the items stored in the application is a versatile tool that deserves some attention. The user can sort by columns using the grids customizable interface. The Grid also has powerful search capabilities as well as the ability to export its data to a number of formats including Excel and PDF.

CLEAR USER CACHE

Clear User Cache button (image 3.3) will revert all adjustments and customization that you have made for your user regarding the user grid, this reloads layout of tables, filters, etc. This function will not reset any data that has been entered or edited in the grid.

GROUPING BY COLUMN

The Grid allows the user to drag a column to a grouping area placed above the column titles (image 3.5) and sort the contents of the grid into groups based on the column selected. To revert to the default list you must only drag all grouped columns back out of the group-by area. This should return the Grid to its original state.

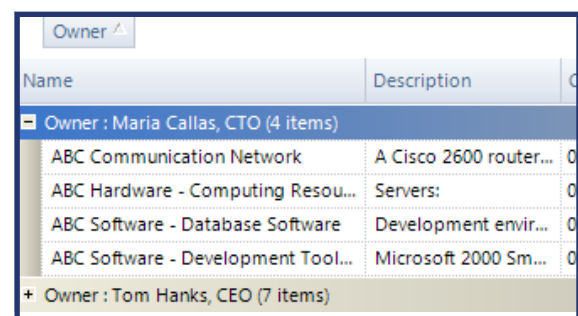


Image 3.5 - Sort By Column

To revert to the default list you must drag all grouped columns back out of the group-by area. This should return the Grid to its original state.

GROUPING BY SUBCATEGORIES

The user can also group by sub categories once a list has been sorted by a specific column (image 3.6).

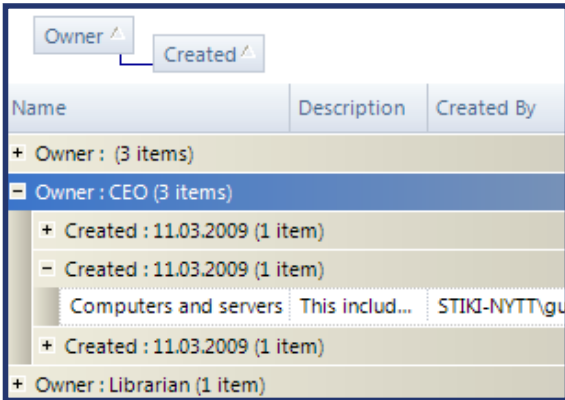


Image 3.6 - Sort By Sub Category

This works in the same way as grouping by a single column. The user need only drag the next column they wish to sub categorize by into the group-by area next to the current grouped-by column (image 3.6).

POWERFUL SEARCH

The Grid offers the User the capability to search by a variety of criteria. Amongst those are free text search and search by parameters such as “less than” and “equal to” to name a few. To use the search you must click on the Search button found on the Toolbar (image 3.7).



Image 3.7 - Toolbar

If you click on the drop down box you can choose which criteria you wish to search by (image 3.8).

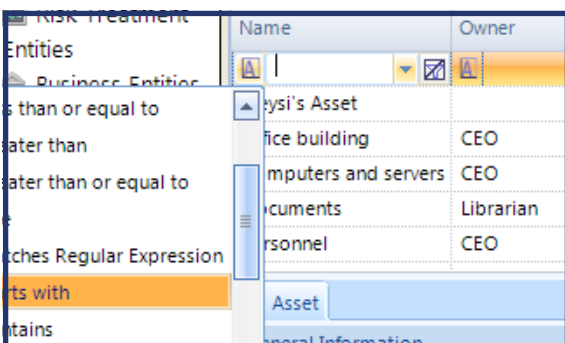


Image 3.8 - Search

EXPORT FACILITIES

All the lists can be exported to Excel and Portable Document Format (PDF). To do this you must use the buttons with the appropriate icons on the Toolbar (image 3.9).



Image 3.9 - Toolbar

4. INTRODUCTION

The **Risk Management** part of RM Studio® consists of several solution items, referred to as Processes. Underlying each Process is one or more Entities.

ENTITIES

BUSINESS ENTITIES

Here is the list of every Business Entity in the system and here new ones are added to the system (image 4.1).

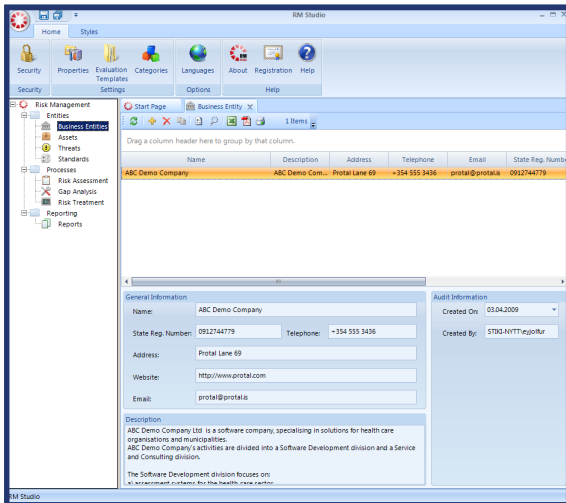


Image 4.1 - Business Entities

ASSETS

Before you can start working with Assessments you will have to define your Assets (as it is the Assets which are being assessed). When you work with an Assessment you will retrieve the Assets pertaining to that Assessment from here (image 4.2).

THREATS

This section contains all Threats defined in RM Studio®. RM Studio® comes with a complete set of predefined Threats, covering most of the Risks you would expect to run into when assessing information security. You can modify or define any Threats that you need for other objects that are up for assessment in RM Studio®. Create new Threats by clicking on the New Threat

button (image 4.3).

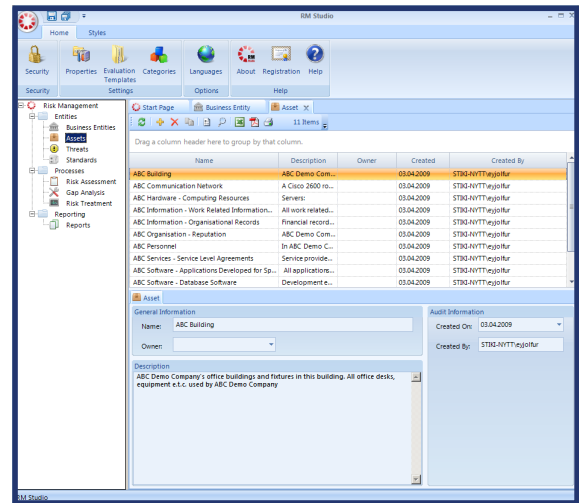


Image 4.2 - Assets



Image 4.3 - the Toolbar

STANDARDS

This section contains the code of practice, i.e. all the Standard clauses and the implementation guide for each. The user may add a custom Standard and format the Standard clauses according to its structure. The controls from a Standard are used in the Risk Management Process. A user defined Standard can be grouped into header sections and subsections. New user defined Standards are inserted by clicking the single plus signs and new Controls are inserted by clicking the double plus sign.

You can also buy fully implemented standards from Stiki. Which are ready for deployment. You will get a license key from Stiki which will unlock the Standard you bought and make it available in RM Studio (image 4.4a).

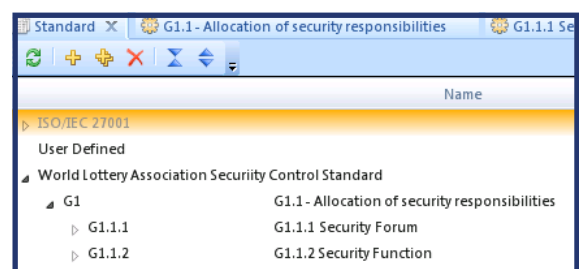


Image 4.4 - Standards and Controls

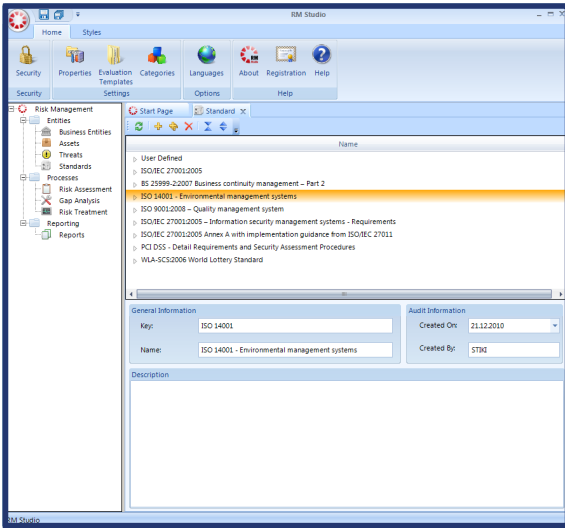


Image 4.4a - Deployed Standards

PROCESSES

RISK ASSESSMENT

The first Process module is the Risk Assessment, which contains all Assessments that have been performed.

An Assessment is an evaluation of all Assets in the organization in regards to their selected evaluation factors. The Standard factors are Confidentiality, Integrity and Availability. An Assessment also takes into account which Risks are relevant to those Assets and the Impact & Probability of the related Threats along with the Vulnerability of the Asset in light of that Threat.

GAP ANALYSIS

The second Process module is Gap Analysis. Gap Analysis is an assessment tool enabling the user to compare their actual state in regards to a particular Standard with what is needed to be eligible for certification. Gap Analysis answers two questions:

- ▲ Where are we?
- ▲ Where do we want to be?

The Gap Analysis is typically done as a precursor to the certification process. A Gap Analysis will reveal how much of a given Standard your organization currently complies to.

RISK TREATMENT

The third Process module is Risk Treatment. Risk Treatment is an integral part of Standard compliance and defines if, how and when you will address the issues that you have defined in earlier steps.

WORKING WITH THE PROCESSES

Having double clicked on one of the Processes, say Risk Assessment, from the navigation tree you are presented with a list of all assessments available in your system (image 4.5). The information will vary slightly between processes but the overall functionality is the same, we will go into further details about each process later on in the Manual. Along with this list you are presented with a pane, found at the bottom of the screen, that provides an overview of the information available for each Process, in this case Assessment (image 4.6).



Image 4.6 - Information Pane

Name	Scope and Basic Criteria	Starts	Ends	Security Risk	Business Entity Name	Created By	Created
V2010	The management of information...	30.08.2010	30.08.2010	60%	Vatnajokull	Administrator	30.08.2010
A2010	The management of information...	31.08.2010	31.08.2010	100%	Vatnajokull	STIK-NYTT:sigu...	31.08.2010
B2010	The management of information...	31.08.2010	31.08.2010	60%	Vatnajokull	STIK-NYTT:sigu...	31.08.2010
A2010 - version 2.0	The management of information...	31.08.2010	31.08.2010	100%	Vatnajokull	Administrator	01.09.2010
Firewall	The management of information...	31.08.2010	31.08.2010	100%	Vatnajokull	Administrator	31.08.2010

Image 4.5 - List of Assessments

When you run the program for the first time there will be no defined process entities in the database so each list will be empty.

If the list is populated you can reopen any Process item by choosing it in the relevant list, the relevant information will then be presented on the information pane. As discussed before in the Navigation chapter, to work with an individual process element you must double click on the item to have it opened in a separate tab.

REPORTING

REPORTS

RM Studio® offers a variety of reporting possibilities. This gives the user a clearer, more detailed overview of the Risk Management. RM Studio® reports use Microsoft Reporting Server and users can define their own reports using Reporting Services.

Asset	Description
ABC Building	ABC Demo Company's office buildings and fixtures in this building. All office desks, equipment e.t.c. used by ABC Demo Company.

Security Risk	Confidentiality	Integrity	Value	Vulnerability of Asset
30%	Medium	High	Very High	Very High

Threat Name	Availability	Impact of Threat	Probability of Threat
Accidental damage - extremes of temperature / humidity	Very High	Medium	High
Accidental damage - fire	Immense	Medium	Immense
Accidental damage - water / soiling	High	Medium	Medium

Image 4.7 - Example of a Report

5. BUSINESS ENTITIES

PURPOSE

Define Entities to use in Assessment & GAP Analysis

PREREQUISITES

None

STARTING TO USE RM STUDIO®

The first thing you need to do when using RM Studio® is to define your Business Entities.

A Business Entity can be a whole organization or part thereof. It can also be many other things, e.g. a different company, a client, case or a scenario. All Assessments and GAP Analysis are made for a specific Business Entity, Risk Treatments are done for a specific Assessment so before you start you have to define the Business Entities you are going to work with.

Under Business Entities, you can view a list of all Business Entities in the system and create new ones (image 5.1).

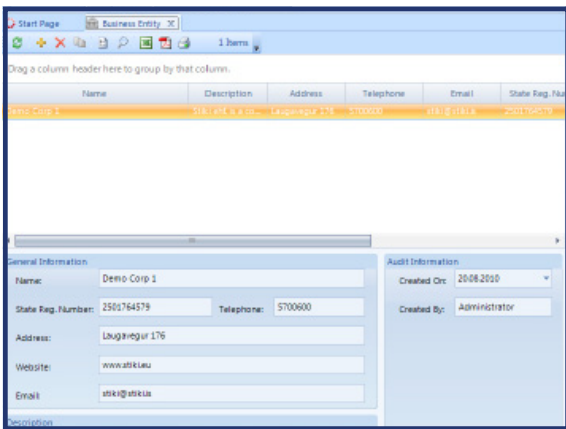


Image 5.1 - Business Entities

CREATING A NEW BUSINESS ENTITY

To create a new Business Entity you must

click on the Add New Business Entity button on the Business Entity Toolbar (image 5.2).

For each new Business Entity, you can define the detail information for the Business Entity (image 5.3).



Image 5.2 - Toolbar

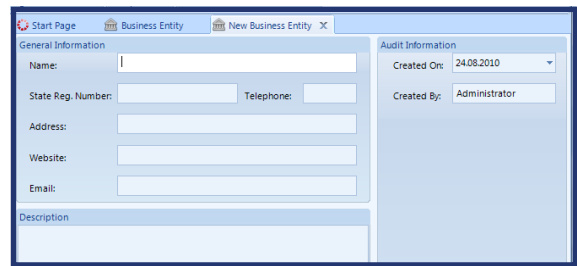


Image 5.3 - Business Entity Information

When you have defined your Business Entity remember to press the Save Button (image 5.4).

It is a good idea to regularly save your work to ensure that you don't lose any data.

You can now use your Business Entity in an Assessment.



Image 5.4 - Save Button

SAVING YOUR WORK

In the upper left hand corner of RM Studio® you will find the Save buttons (image 5.4). The one on the left is for saving the work on the current tab. The one on the right is a cascading Save button that will save all unsaved data in all open tabs.

6. ASSETS

PURPOSE

Define Assets to use in Assessments, uses Categories to connect Assets & Threats.

PREREQUISITES

None

WHAT ARE ASSETS

Assets are anything that has value to the organization according to the Standard. Assets are therefore the building blocks around which you build an Assessment. They can be as general as “A Building” or as specific as “HP Server named XV-231”. You will define your own Assets. An Asset can be defined as anything of value to the organization.

Under Assets you will only define what the Assets are, you will not define their value to your organization until later when you begin an Assessment.

Assets are defined once in the Asset List (image 6.1) and can then be reused across multiple Assessments.

DEFINING ASSETS

To define your company’s Assets you must go to the Asset List by double clicking on Assets in the navigation tree on the left hand side of the RM Studio® window.

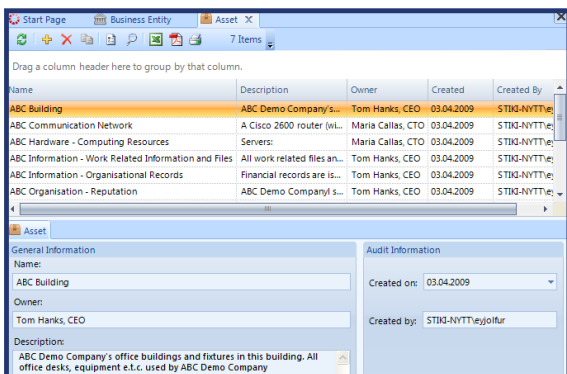


Image 6.1 - Assets

CREATING A NEW ASSET

To add a new Asset you must click on the Add New Asset icon (image 6.2) on the Asset List Toolbar.



Image 6.2 - Toolbar

A New Asset tab will open (image 6.3). Here you will define all the relevant information for the Asset in question.

In the Categories Tab you can categorize the Asset. You can have the Asset in several different Categories.

It is very important to specify the Asset Category as it is a prerequisite for using it in an Assessment, and is the basis for identifying the Threats associated with the Asset.

Assets can not be created unless an owner is assigned to the asset.

See further “Owner” on page 29

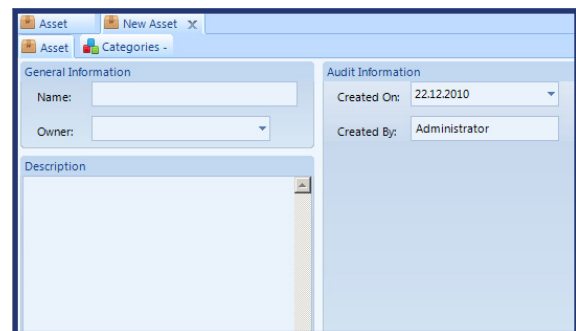


Image 6.3 - New Asset

DESCRIPTION

The Description text box (image 6.3) gives you the possibility to describe in detail the Asset in question. In this field we encourage our users to give a thorough description so that later users will have an insight into the reasoning behind any given Asset.

CATEGORIES

To Categorize the Asset you must click on

the Add New Category icon (image 6.2) in the Categories List Toolbar. You will be presented with a list (image 6.4) from which you can choose the appropriate Category.

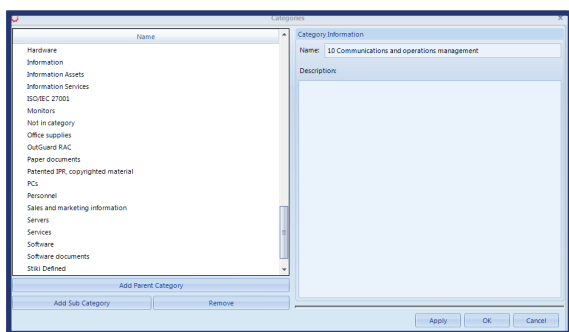


Image 6.4 - Categories

The Categories are important for the calculations of the Information Security Risk. They are used to connect Assets with Threats in a relationship that is defined as “Risk”.

In the case when you can not find the appropriate Category or Sub Category, you can add both to meet your specifications.

When this is done the Assets can then be used in an Assessment.

WORKING WITH ASSETS - NEW FEATURE

Our latest addition to the grid is that the user can now make multiple changes by selecting the rows he wants to change values for to the same status and right-click on the selection.

When a user right-clicks (image 6.5) the available options in the Assets are for the user with sufficient rights to, Delete the Asset, Copy the Asset and change the Owner of the Asset.

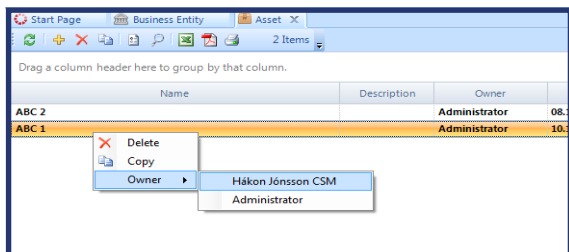


Image 6.5 - Multiple changes

RISK IS A RELATIONSHIP

The Categories are important for the calculations of the Information Security Risk. They are used to connect Assets with Threats in a relationship that is defined as “Risk”.

7. THREATS

PURPOSE

Define Threats that can harm given Assets (via Categories) + define mitigating Controls.

PREREQUISITES

None

The Stiki Pre-entered Data license allows you to use the 149 Threats that are bundled with RM Studio®, these are Threats defined by Stiki's inhouse experts. Although the 149 Threats cover the vast majority of the Risks you would expect to run into, you can also create new Threats by clicking on the New Threat button (image 10.1).

All Stiki defined Threats can be modified and adjusted to your business and environment. This includes changes to associations with categories and mitigating controls.



Image 10.1 - Toolbar

CREATING A NEW THREAT

When creating a new Threat the first thing you do is give it a name. The more precise the name the better it is for other people to use. Have this in mind also when you write the description of the Threat (image 10.2).

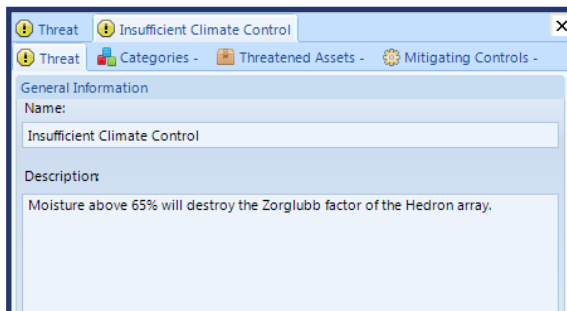


Image 10.2 - Threat

CATEGORIES

To assign the Threat to a Category navigate to the Category tab and click on the "Add New Categories" icon (image 10.1). You will then be presented with a list of Categories (image 10.3). Select one Category and click the OK button to assign it to the Threat.

You can add more Categories to a Threat by repeating these steps.

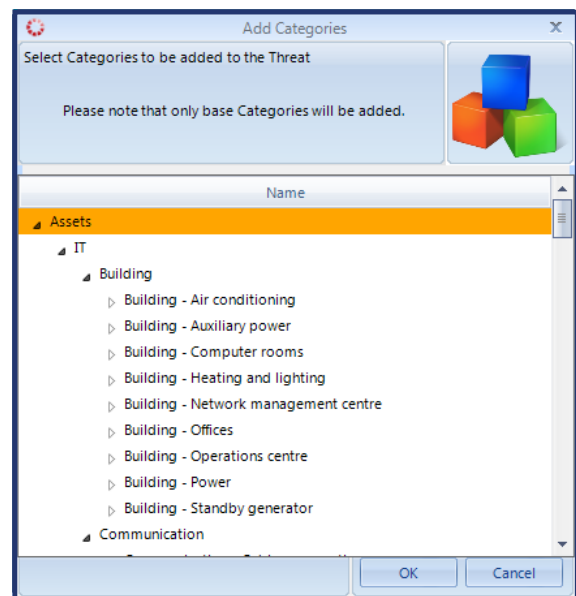


Image 10.3 - Categories

THREATENED ASSETS

The Threatened Assets tab aggregates all the Assets from all the Assessments that have been marked as threatened by the respective Threats.

MITIGATING CONTROLS

Under Mitigating Controls you can define which Controls work against a given Threat. To add a new Mitigating Control from the Control list you must click on the "Add New Mitigating Control" icon on the Mitigating Controls Toolbar (image 10.1).

8. STANDARDS

PURPOSE

Define Standards that can neutralize given Threats.

PREREQUISITES

Keys to the Standards that need deployment

Stiki is now offering users 9 Pre-entered Standards with Controls. This is a major change since the last release (v2.3) and the deployment of the Standards has changed a little bit.

When a user purchases the software he/she will have to choose one of the Standards that Stiki offers. The license Stiki will issue upon purchase will unlock the Standard you bought and the languages needed.

AVAILABLE STANDARDS

- ISO/IEC 27001:2005
- ISO 14001 - Environmental management systems
- ISO 9001:2008 – Quality management system
- BS 25999-2:2007 Business continuity management – Part 2
- ISO/IEC 27001:2005 – Information security management systems - Requirements
- ISO/IEC 27001:2005 Annex A with implementation guidance from ISO/IEC 27011
- PCI DSS - Detail Requirements and Security Assessment Procedures
- WLA-SCS:2006 World Lottery Standard

HOW TO INSTALL A STANDARD

The user does not need to create the Standard in the system as in previous versions. Previously Stiki only offered the ISO/IEC 27001 Standard. To open up the desired Standard you need to enter the Properties > Standard Data (image 11.1)

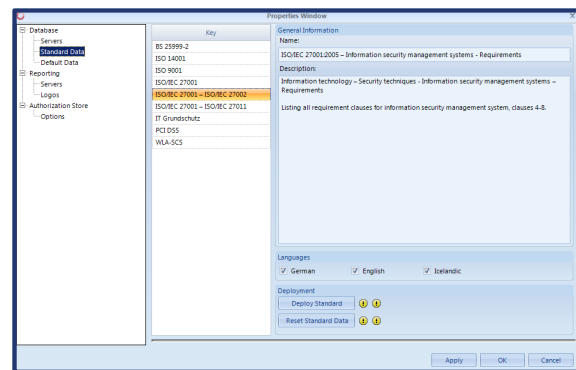


Image 11.1 - Standard Deployment

The Standards that are available to you will be in dark font while the others that are not available are grayed out.

Select the Standard you would like to deploy and start to use > Select the languages you would like for the Standards and press **Deploy Standard** (image 11.2)

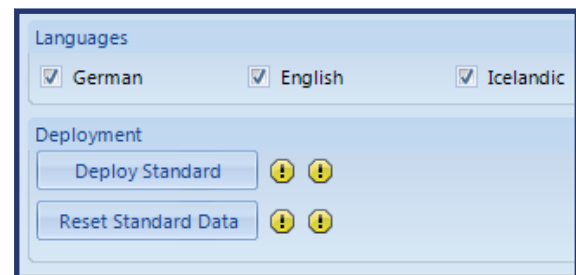


Image 11.2 - Deploy Standard

This process needs to be done for all the Standards you would like to deploy into RM Studio.

RESET STANDARD DATA

The Reset Standard Data button will roll-back every change made to the deployed

Standard and revert it to the original state.

This will however not revert the User Defined Controls.

STANDARD CONTROLS

You can define your own Standards in addition to the ones offered by Stiki and thus Controls by clicking on the “Add New Standard” icon on the menu bar (image 11.3)



Image 11.3 - Toolbar

You can add a Standard name and create subsections (Children) by clicking the double plus sign „New Child“.

By ticking the Group Header box next to the Control number you create a Header where multiple „children“ can be added under.

General Information

Control Number: Group Header

Name:

Standard:

Implementation Guide

Appendix 1 – General Security: WLA Basic Controls

The list below contains the required controls that shall be implemented in organizations to become WLA certified. This is in addition to those controls defined in ISO 27001 Annex A and shall be part of the organization's Information Security Management System (ISMS).

Image 11.4 - Group Header

WORKING WITH THE CONTROLS

The Standard Controls bundled with RM Studio®, can be edited. This should be handled with care and only done to adjust the controls to the environment you will be auditing. You can revert to the default library by Resetting the Default Data in the Properties Window under Standard Date - **Reset Standard Data** (see p. 35).

CREATING NEW STADARDS AND CONTROLS

When creating a new Standard or Control the user will have to give the item a number and a name.

The user should then write an Implementation Guide that is as thorough as possible. A thorough, clear and concise Implementation Guide will ensure that the Standard or Control is used in the same way

every time (image 11.5).

General Information

Control Number: Group Header

Name:

Standard:

Audit Information

Created On:

Created By:

Implementation Guide

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc hendrerit tempor bibendum. Maecenas et eros nunc, et malesuada lacus. Nulla sit amet varius purus. Praesent tincidunt tortor vel neque vehicula ultricies. Vestibulum eget lobortis nisi. Ut ac dolor a urna pretium sagittis at at nisi. Aenean augue nibh, commodo a feugiat nec, rhoncus quis odio. Vestibulum lacinia, lacus et porttitor vehicula, ipsum nisi dapibus lorem, a pellentesque neque nisi at nulla. Curabitur non velit ante, eget mattis turpis. Nulla malesuada lacus justo, ac lacinia metus facilisis ac. Aenean ultricies dolor in augue dignissim lobortis. Vestibulum pellentesque sapien eu risus congue sagittis. Nulla ullamcorper mauris sit amet nibh ornare elementum. Phasellus ut purus ac ligula aliquam fermentum sit amet sed ligula. Suspendisse nec enim at nulla pulvinar tempor. Curabitur eleifend tortor vitae lorem venenatis aliquam.

Image 11.5 - Implementation

9. REPORTS

REPORTS



PURPOSE

Generate Low or High Level Reports from given Processes.

PREREQUISITES

Predefined Report Templates and Microsoft Reporting Services are correctly installed and connected to RM Studio®

RM Studio® offers a variety of reports. You can view them on screen, print or save them in a variety of formats including PDF, Excel and Word.

THE STANDARD REPORTS:

- **Statement of Applicability (SOA):** the Statement of Applicability report is an overview of the status of the Risk Treatment. A Statement of Applicability is a list of all Controls from the Standard used to perform the Risk Treatment which have been labelled as Implemented, Not Implemented, Future Controls or Not Applicable. The descriptions entered for each respective control are also printed out. The status of the Risk Treatment is also displayed graphically. The report is useful for the managers of business units, customers, and agencies, e.g. the Data Protection Authority, which require a declaration of the security of the Risk Treatment in question. It can also be submitted to auditors.
- **Risk Assessment - Detailed information:** the Assessment report contains all information entered into RM Studio® for the Assessment in question.
- **Risk Treatment - Future controls (simple report):** this report provides an overview of all Future Controls that have been defined for a given Risk Treatment. They are ranked according to date, so that the Control with the earliest date of implementation is shown first.
- **GAP Analysis - Future controls (simple report):** this report provides an overview of all Future Controls that have been defined for a given GAP Analysis. They are ranked according to date, so that the Control with the earliest date of implementation is shown first.
- **Assets with Threats:** Like the name indicates the Assets with Threats report aggregates all the Assets from a single Assessment and their respective threats. For each Asset the report states which values the Asset Evaluation Values and Threat Evaluation Values have¹. The report also states the Security Risk for each Asset.
- **Asset with Controls:** This report shows all Assets in Assessment and the Controls used to mitigate their risks. The user can see all controls from the ISO/IEC 27001 Standard as well as any user defined Controls. The status of implementation of each controls is also shown.
- **Executive Summary:** Shows the most important Assets based on the CIA values (Confidentiality, Integrity and Availability). It also shows the most Valuable Assets. The user can choose the number of Assets to be reported. The Executive Summary report is a great overview of Security Risk and Ratio of Controls. All calculations are shown graphically in a color coded way and gives the management key information on a single sheet.
- **Risk Treatment:** All risks are listed along with their base, current and future security risk. the list is grouped by

¹ The Definition of Evaluation Values you can find in chapter 13.

the Risk Treatment. Users can sort Risks by Base Security Risk, Current Security Risk, or Future Security Risk. This report provides a total overview of the risks and the treatment for each of them.

NEW REPORTS

- **Controls With Assets:** This report will show you all the Controls in your Risk Treatment, the name of the Control, Status of the Control, and Assets associated with the Control.
- **Gap Analysis - Results:** This report is basically the same report as the SoA which is generated from the Risk Treatment results. This report allows you to generate the same report based on Gap Analysis.
- **Risk With Controls:** This report is only available to those using the Local Reports. This report is useful when information is needed on whether or not a control has been implemented for specific risks (image 12.1).

Risks with Controls		ABC Demo Risk Treatment		Stiki Information Security	
Statuses Included					
Implemented					
Future control					
Partly implemented					
Not applicable					
Not implemented					
Threat		Asset		Number	
Abuse of security measures – 'tailgating', misuse of access tokens, etc		ABC Building		6	
Control Number	Control	Status	Implemented		
5.1.1	Information security policy document	Implemented	03/04/200		
5.1.2	Review of the information security policy	Future Control	03/04/200		
6.1.1	Management commitment to information security	Implemented	03/04/200		
6.1.2	Information security co-ordination	Implemented	03/04/200		
6.1.3	Allocation of information security responsibilities	Implemented	03/04/200		

Image 12.1 - Risks with Controls

10. RISK ASSESSMENTS

PURPOSE

Calculate Base Information Security Risk for the Scope of the Assessment.

PREREQUISITES

Business Entity and Asset(s) have been defined.

WORKING WITH ASSESSMENTS

Assessment is the process you use to assess the level of Base Information Security Risk for your Business Entity. Assessments identify and evaluate Assets and the Risks associated with them. A Risk is defined as the relationship between an Asset and a Threat.

An Assessment will give you an overview of the collective Risks in a Business Entity.

CREATING AN ASSESSMENT

You can create a new Assessment from scratch or continue with an Assessment already in the system. A new version will be created each time you save the Assessments and you can, via version history, view previous versions.

To create a new Assessment you must click on the “Add new Assessment” icon (image 7.1) in the Assessments List toolbar.

The following window (image 7.2) will then appear.



Image 7.1 - Toolbar - Add, Delete and Copy

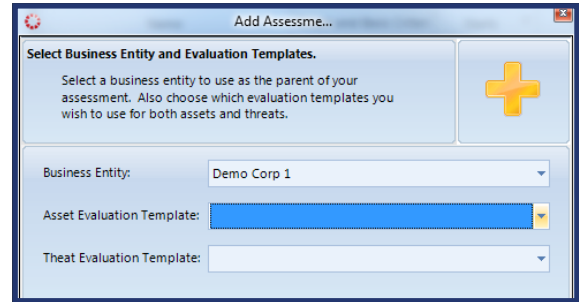


Image 7.2 - Select Business Entity

Having chosen the Business Entity and the Evaluation Templates that you wish to work with in the Assessment click “OK” and a new Assessment will be created for you.

The Assessment information pane (image 7.3) will show the basic information about your Assessment along with the level of Security Risk.

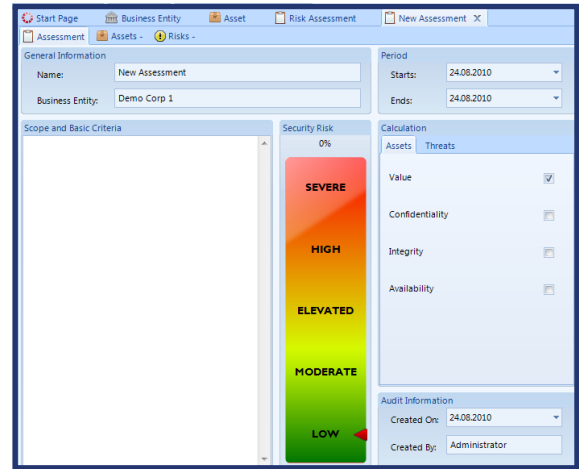


Image 7.3 - Assessment Information

COPY RISK ASSESSMENT

There is a COPY function that enables the user to make a copy of an existing Assessment. This will enable the user to create many versions of the same Assessment. To copy an assessment, right click on the assessment that is to be copied and press copy.

SCOPE AND BASIC CRITERIA

In the Scope and Basic Criteria field you will enter the defined Scope for your Assessment along with the Basic Criteria that you have

given yourself.

The Scope will define all the aspects that you will take into account when doing your Assessment.

The Basic Criteria will state how much Risk you are willing to accept i.e. the minimum level of Risk.

EXAMPLE OF BASIC CRITERIA

Risk Criteria

According to the Standard ISO/IEC 27001:2005

Risk Assessment approach and criteria

For Risk Assessment according to the Standard: ISO/IEC 27001:2005 Information Technology - Secure Techniques - Information Security Management Systems - Requirements.

In accordance to Fritz & Son's information security policy, accepted in March 2009. Fritz & Son's security forum has approved the method used in RM Studio® Risk Assessment process for use in Risk Assessments at Fritz & Son. Information assets have been defined as group assets. Value of assets has been assessed as well as their properties regarding confidentiality, integrity and availability (CIA). Threats to assets have been identified, the probability of occurrence and impact have been estimated. Vulnerability of assets towards a threat has also been estimated.

In this method the risk calculations is based on the following evaluations:

- The value of the asset
- The probability of a specific threat
- The impact of the threat
- The vulnerability of the Asset

Base Security risk is the real risk as evaluated by the user regarding the 4 variables through a 4th dimensional matrix.

WORKING WITH ASSETS

Under the Assets tab you will find a lists of all the Assets relevant to the selected Assessment (image 7.4).

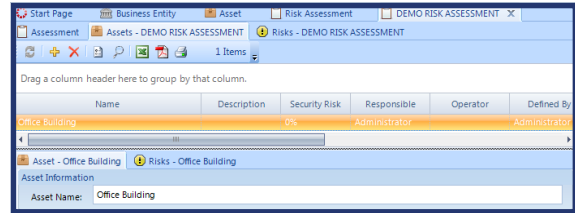


Image 7.4 - Assets

The next step in the Risk Assessment process is the definition of the Information Assets to be assessed. You can add Assets by clicking on the “Add new Asset” icon on the Asset List Toolbar (image 7.5).



Image 7.5 - Toolbar

ASSETS RETRIEVED

When you have clicked the “Add new Asset” icon on the Asset List Toolbar (image 7.5) you are presented with a list (image 7.6) of all the Assets that you have defined under the Asset Entity of RM Studio® (chapter 6). From the list choose the Assets that are relevant to the Assessment by highlighting them and clicking on the “OK” button (image 7.6).

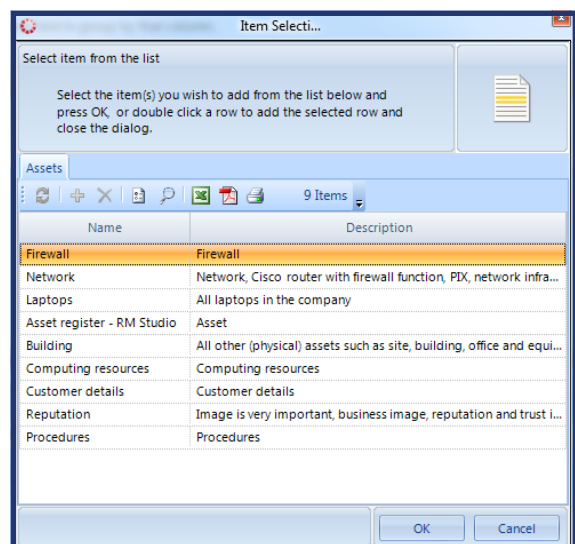


Image 7.6 - Asset selection

OWNER

According to the ISO 27002 Standard, a Responsible Person must be registered for all information Assets in addition to assessing their Confidentiality, Integrity and Availability. The Responsible Person cannot

be the Business Entity itself, but must be a specific individual who is registered under a name or job position.

The Responsible Person is selected from a drop down list of registered users (see the Security section of chapter 2) on the Asset's Information tab (image 7.7).

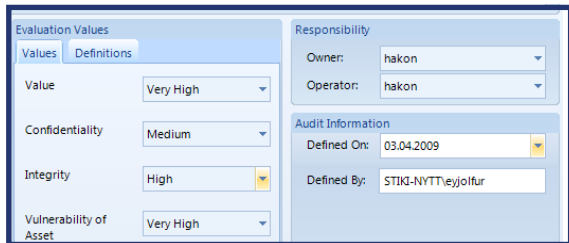


Image 7.7 - Asset Information

OPERATOR

The Responsible Person and the Operator need not be the same person. The Operator is also selected from a drop down list of registered users (see the Security section of chapter 2) on the Asset's Information tab (image 7.7).

The System Administrator can be the Operator, while the head of the IT division is the person Responsible for the Asset.

EVALUATION VALUES

The evaluation template chosen upon assessment creation defines the properties that need to be evaluated.

If you are using the Standard Evaluation Template the properties to evaluate are Asset Value, Integrity and Availability. The possible values for the properties are Immense, Very High, High, Medium or Low. The definitions of these terms can be found in the Definitions of Asset Properties (chapter 13) and can be adjusted as needed via the Evaluation Templates. It is important to review and adjust the definitions to ensure that the results are always the same when Risk Assessments are repeated.

The value of the Properties are set on the details pane (Asset Tab) of each individual Asset in the Assessment (image 7.8).

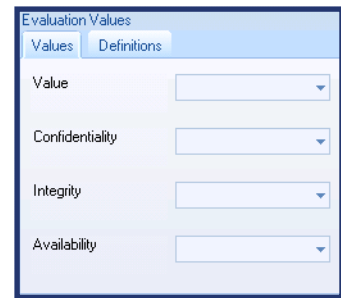


Image 7.8 - Evaluation Values

CONFIDENTIALITY

How important the Confidentiality of a particular Asset is to the organization must be qualified. An example would be that a server has an Immense value while an office would have a high one.

INTEGRITY

The value of Integrity is based on how important the correctness of the given Information Asset is to the company. An example would be that a certain file or database is of Immense value while another has a low one.

AVAILABILITY

The value of Availability is based on how important it is for the organization to have the Asset readily available. An example could be that the Office has an Very High value while an archive has a Medium value.

VALUE

The Value of the Asset must be assessed. This Value is used when calculating Security Risks. The Value of the Asset can be Immense, Very High, High, Medium, or Low. It is important to specify definitions to ensure that the results are always the same when Risk Assessments are repeated (image 7.8).

DEFINITIONS OF VALUE AND PROPERTIES

Some examples of definitions of value and properties have been entered in advance. These can be adjusted as needed via the Evaluation Templates. It is important to specify definitions to ensure that the results are always the same when risk assessments are repeated, even by different people. However, these definitions can be changed.

RISKS

For each Asset there is a Risk Tab. This tab is located below the Asset List (image 7.4). Here you will find a list with all the Risks associated with an individual Asset depending on how the Asset has been Categorized.

ADDING RISKS

To add a risk to an Asset you must click on the “Add new Risk” icon on the Risk List Toolbar (image 7.9).



Image 7.9 - Toolbar

AGGREGATED VIEW OF RISKS

Next to the Asset List Tab, located above the Asset List there is another Risk Tab (image 7.10). On this tab there is a list that aggregates all the Risks associated with all the Assets in the individual Assessment.

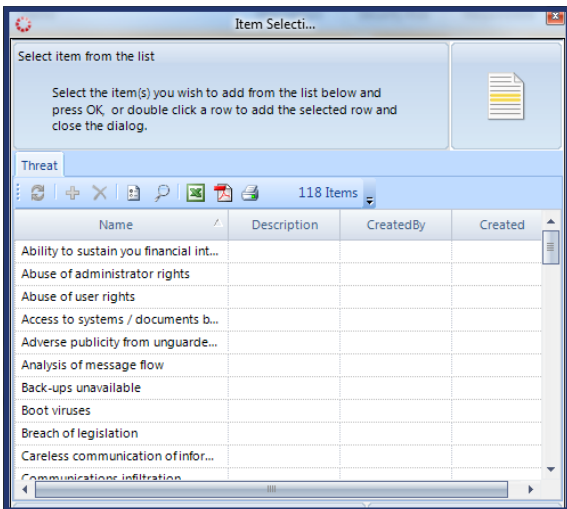


Image 7.10 - Threat selection

RELATIONSHIP BETWEEN ASSETS AND THREATS

RM Studio® contains a database of Threats. If you want to create a new Threat at this point, then you must first save and close the current Assessment before creating a “New Threat” in the Threat entity of RM Studio®. We’ll discuss Threats in more detail later in chapter 10.

- Each Threat must be examined. If you do not agree that a Threat is imminent, you can delete it by highlighting the Risk, and either hitting the delete key or right

clicking and selecting delete from the context menu.

- Enter information in the Description window to support the Assessment.

PROPERTIES

The values registered for the properties of the Threat are used for calculating the Security Risk. In the Standard Evaluation Template the properties are: Impact, Probability and Vulnerability. The values for each of the properties can be defined as Immense, Very High, High, Medium or Low. The definitions of the terms can be found in the Definitions of Threat Properties (chapter 13).

The properties and their values can be adjusted as needed via the Evaluation Templates. For more information see chapter 2.

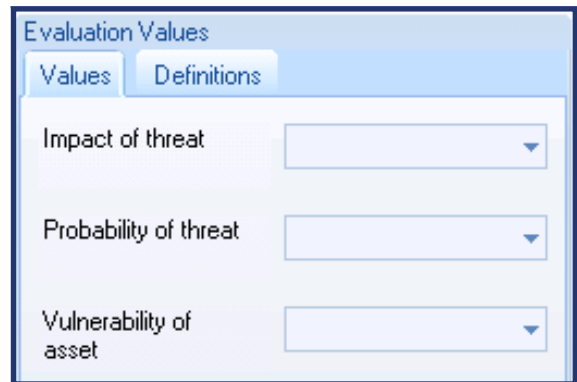


Image 7.11 - Setting Property Value

IMPACT OF THREAT

The Impact of Threat property assesses how serious the consequences are should the Threat occur.

PROBABILITY OF THREAT

The Probability of Threat property dictates how likely a Threat is to occur.

VULNERABILITY OF ASSET

The Vulnerability of Asset property evaluates how vulnerable the Asset is to the Threat.



Image 7.12 - Save Button

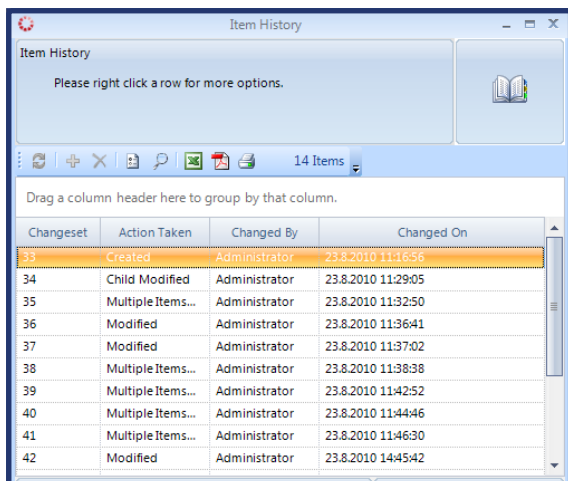
HISTORY

RM Studio® provides powerful traceability capabilities, with a complete version history on Risk Assessments. Users can now call up a version history for any Assessment and view previous versions as a whole or dig down into the individual building blocks of the Assessment, such as Assets and Risks. The version history will be applied to other elements of RM Studio® and made even more powerful in our future releases.

ITEM HISTORY

If you right-click on a Risk Assessment, an Asset in Assessment, or a Risk, you can choose History from the context menu. This will bring up the Item History window (image 7.13). This window shows the entire history for this particular item. You will see the ID of the Changeset associated with the history entry, the action taken, who performed the action and when.

If you then right click on any entry in the Item History window, you can choose “View Item”, “Changeset details”, and if you are viewing the item history for an Assessment, you can choose “View Assessment version”.



The Item History window displays a table with the following columns: Changeset, Action Taken, Changed By, and Changed On. The table contains 14 rows of data, with the first row highlighted in orange.

Changeset	Action Taken	Changed By	Changed On
33	Created	Administrator	23.8.2010 11:16:56
34	Child Modified	Administrator	23.8.2010 11:29:05
35	Multiple Items...	Administrator	23.8.2010 11:32:50
36	Modified	Administrator	23.8.2010 11:36:41
37	Modified	Administrator	23.8.2010 11:37:02
38	Multiple Items...	Administrator	23.8.2010 11:38:38
39	Multiple Items...	Administrator	23.8.2010 11:42:52
40	Multiple Items...	Administrator	23.8.2010 11:44:46
41	Multiple Items...	Administrator	23.8.2010 11:46:30
42	Modified	Administrator	23.8.2010 14:45:42

Image 7.13 - Item History

VIEW ITEM

This window shows the information associated with a particular item at a particular time in its history. Note that it will show only the information directly related to the item. For example, if you choose to “View Item” on an Asset, it will only show the asset information, not the

risks connected to the asset. If you wish to view that relationship in a history entry, use the “View Assessment version” option from the “Item History” window for an Assessment.

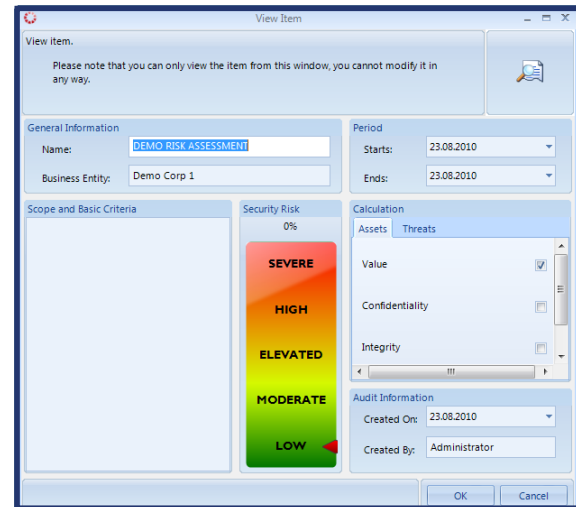


Image 7.14 - View Item

CHANGESET DETAILS

Each action taken on an Assessment is grouped together into a changeset. A single changeset is created when you save an Assessment. So if you open an Assessment, add 2 Assets (and several risks that get added automatically), change the evaluation on several other Assets, remove one, and edit the scope of the Assessment, all of these actions will be grouped together in one changeset. By choosing a single history entry and clicking on “Changeset details” you can view all the other actions performed at the same time as that single entry. This window shows the changeset ID, the action taken, the name of the object affected, and the type of the object affected. From here you can also view the specific item.

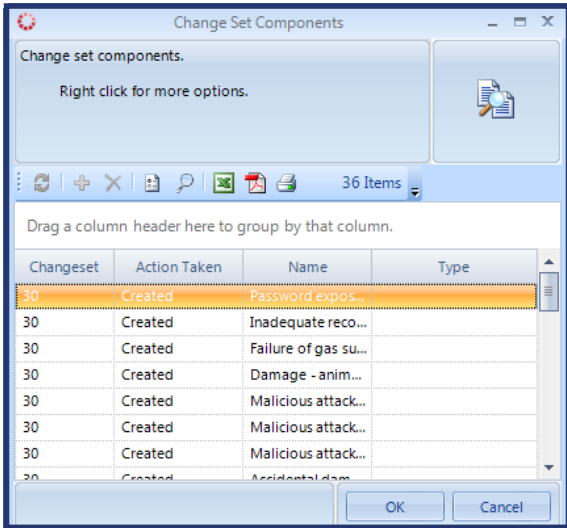


Image 7.15 - Change Set Components

VIEW RISK ASSESSMENT VERSION

This window shows a snapshot of the entire Assessment at any given time in its history. This includes all Assets and Risks, including their evaluations.

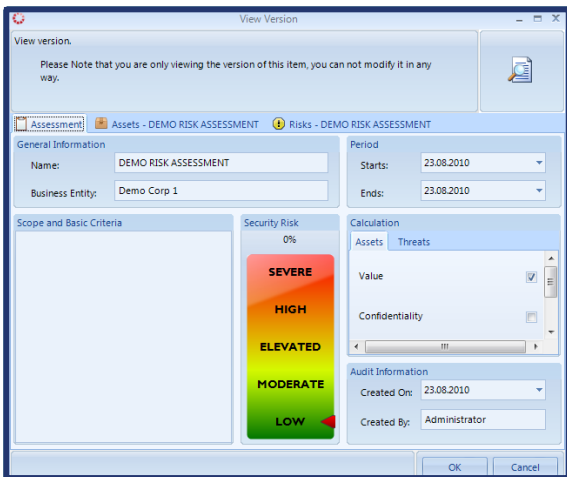


Image 7.16 - View Version

RIGHT - CLICK OPTION

Our latest addition to the grid is that the user can now make multiple changes by selecting the rows he wants to change values for to the same status and right-click on the selection.

When a user right-clicks (image 7.17) the available options in the Asset list are for the user with sufficient rights to, Delete the Asset, change the Value of the Assets, Confidentiality, Integrity, Availability, who is responsible and who is the owner of the Asset.

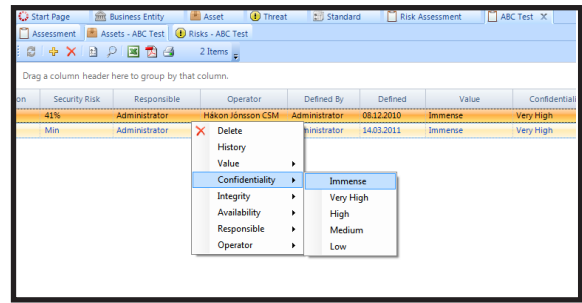


Image 7.17 - Right-Click on Asset list in Risk Assessment.

II. GAP ANALYSIS

PURPOSE

Set Implementation Status of each Control on global level.

PREREQUISITES

Business Entity

Gap Analysis is an assessment tool enabling the user to compare their actual state in regards to a particular Standard with what is needed to be eligible for certification.

That is to say, that the status and necessity of the controls defined in the relevant Standard are evaluated.

CREATING A NEW GAP ANALYSIS

A Gap Analysis is made on a particular Standard for a particular Business Entity. So the first thing to do when creating a new Gap Analysis is to select the appropriate Standard and Business Entity (image 8.1). Creating Business Entities was discussed in the chapter 5.

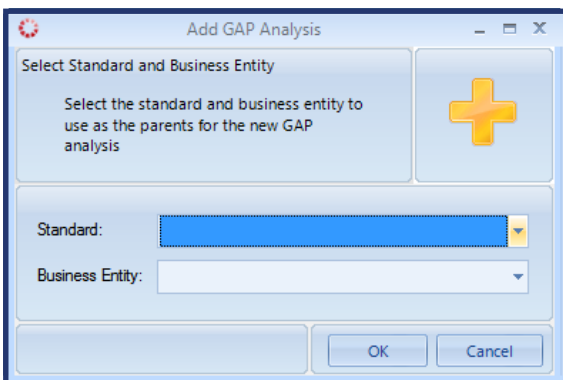


Image 8.1 - New GAP Analysis

GAP ANALYSIS INFORMATION

After you have selected the Standard you wish to work with along with the Business Entity you will be asked to name the Gap Analysis as well as to state the duration of the Gap Analysis (image 8.2).

The Description of the Gap Analysis should be filled in clearly and concisely along with the reasoning for the Analysis.

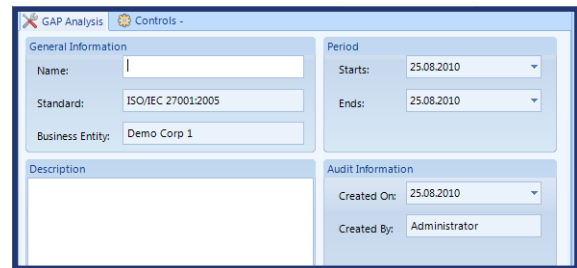


Image 8.2 - GAP Analysis Information

CONTROLS

Under the Controls tab you will find all the Controls from the Standard you chose to work with when you created the Gap Analysis. Below the list of controls you will find the Control Information Pane that lists information about the Control as well as the Implementation Guide for a particular Control (image 8.3).

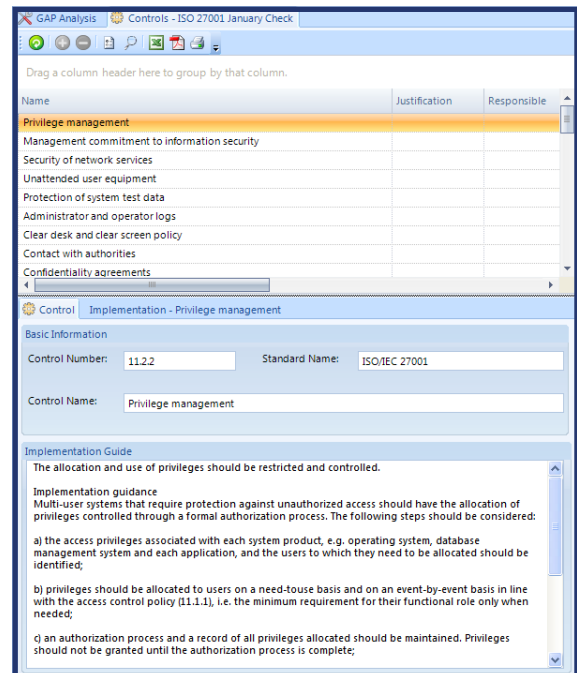


Image 8.3 - Controls

IMPLEMENTATION

Finally, in the Implementation tab, you will define if and how your organization will implement each Control (image 8.4).

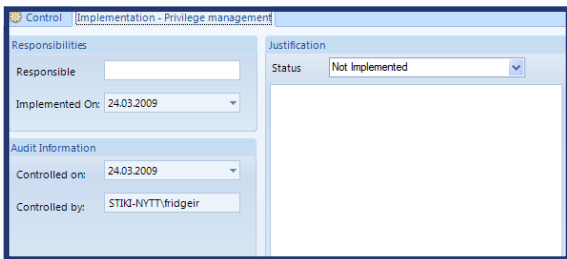


Image 8.4 - Implementation

You can set a responsible person for the implementation of a given Control. To designate a responsible person you must select a registered user from the Responsible drop down box(image 8.5).

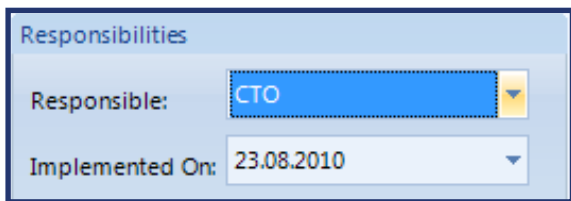


Image 8.5 - Person Responsible

CONTROL STATUS

As you go through the Controls you will decide whether the Control is “Not Applicable” for your organization, If you determine the Control is applicable you must then determine whether it is Not Implemented, Partially Implemented, Fully Implemented, or a Future Control (image 8.6). Future Control means that you plan to Implement the Control at a scheduled time in the future. See more on control status in Right-Clicking.

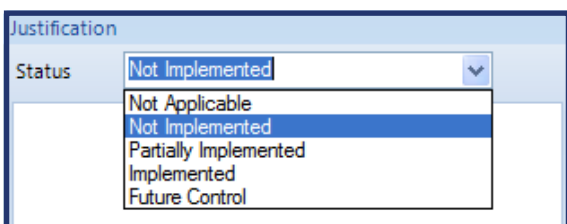


Image 8.6 - Status

RIGHT-CLICKING

Users can now change multiple control statuses by selecting those with the same status and right-click on the selection. The options provided to the user is to change the status of the control and the person responsible for it (image 8.7)

Name	Control Number	Justification	Implemented	Control Status
Privilege management	11.2.2		08.12.2010	Not Implemented
Management commitment to information security	6.1.1		08.12.2010	Not Implemented
Security of network services	10.6.2		08.12.2010	Not Implemented
Unattended user equipment	11.3.2		08.12.2010	Not Implemented
Protection of system test data			08.12.2010	Not Implemented
Administrator and operator logs			08.12.2010	Not Implemented
Protection of log information				Future Control
Protection of information systems audit tools	15.3.2			Implemented
Information security awareness, education, and training	8.2.2			Partially Implemented
Clock synchronization	10.10.6			Not Implemented
Session time-out	11.5.5			Not Applicable
Protecting against external and environmental threats	9.1.4			Not Implemented
Review of user access rights	11.2.4		08.12.2010	Not Implemented

Image 8.7 - Right Clicking

JUSTIFICATION

In the Justification text box you should write the clear and concise reasoning for the defined status of each Control. A thorough Justification will help you later to remember your reasons for giving a Control a particular Status.

12. RISK TREATMENT

PURPOSE

Calculate Current & Future Information Security Risks & manage Risks

PREREQUISITES

Assessment exists and optionally GAP Analysis exists

A Risk Treatment is based on an Assessment. The Risk Treatment calculates the current and future Risk of your organization based on the status of implemented controls and other information from the Assessment.

In the Risk Treatment process you will go through all the Risks that are associated with a particular Assessment and decide how you are going to manage each. You will also decide which controls you are going to use to manage that Risk.

WORKING WITH RISK TREATMENT

When you open the Risk Treatment you are presented with a list of earlier Risk Treatments (image 9.1). To add a new Risk Treatment you must click on the Add New icon on the Risk Treatment Toolbar (image 9.2).



Image 9.2 - Toolbar

You can either work with a new Risk Treatment or you can continue working with an older one. To do this you must double click on a selected Risk Treatment from the Risk Treatment list (image 9.1).

After creating the new Risk Treatment, its information will open in a separate tab (image 9.1). Here you can give a description of the Risk Treatment. The description should be concise and clear so that others can easily understand the reasoning behind the Risk Treatment.

Remember to also fill in the Risk Criteria range. The Risk Criteria is chosen using “Upper Mark” and “Lower Mark” text boxes (image 9.3).

You also set the Period for which the Risk Treatment is valid here.

RISK CRITERIA

By setting the Risk Criteria limits you are deciding which risks fall out of your risk limit.

Period		Risk Criteria	
Starts:	23.08.2010	Upper Mark:	50
Ends:	23.08.2010	Lower Mark:	20

Image 9.3 - Risk Criteria



Image 9.1 - Risk Treatment

Asset Name	Asset Name	Security Risk	Current Security Risk	Future Security Risk	Treatment
- use of arms (act of...	Office Building	10%	10%	10%	
- willful damage / va...	Office Building	10%	9%	9%	
re	Office Building	10%	10%	10%	
ities	Office Building	10%	10%	10%	
nt	Office Building	10%	10%	10%	
ss to utilities	Office Building	10%	10%	10%	

Image 9.4 - Threat List

When the assessor is in the Management tab, he gets a list of all the Threats and below that the details and guides to implement controls.

ASSET LEVEL

To work on the Threats individually you need to select the 'Asset name' column and drag it to the grouping area. By doing so you will now get the option to work on the Asset Level (image 9.5). In the Asset level you are able to set the control status for individual assets, delete controls that are not relevant to the asset, set justification for the status and set the date for future controls. This is a fundamental function that you can only access by grouping assets to the the Asset level.

Name	Asset Name	Control N
Privilege management	Firewall	31.2.2
Management commitment to information security	Firewall	6.1.3
Administrator and operator logs	Firewall	10.10.4
Information labeling and handling	Firewall	7.2.2
Allocation of information security responsibilities	Firewall	6.1.3
Business continuity planning framework	Firewall	14.1.4
Secure disposal or re-use of equipment	Firewall	9.2.6
Documented operating procedures	Firewall	10.1.1

Image 9.5 Asset Level

To be able to set the status for all assets that a single control applies to you need to go to the Controls tab in the top menu (image 9.6).



Image 9.6 Controls Tab

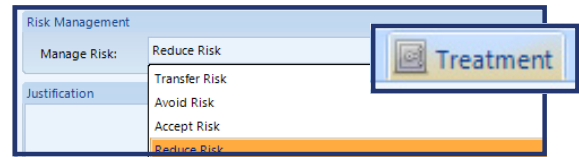


Image 9.7 Risk Management

The only adjustment the assessor can make if he does not access the Asset level is to go through each Risk and decides what action to take. This is done by assigning a state of Transfer Risk, Avoid Risk, Accept Risk or Reduce Risk in the Manage Risk drop down box in the Treatment Tab.

If the assessor chooses to accept the risk, this means that no action was determined necessary. There could be several reasons that no action is thought necessary, one of which might be that the value of the Asset is too low to justify any action. This will require the formal approval from Management.

It is also possible to transfer risks to a third party – an example would be when responsibility is forwarded to an insurance company. A third option would be to avoid risk – an example would be to move operations to another location, e.g. in the event of risks due to earthquakes. A fourth option is to Reduce the risk by implementing controls.

Justifications should always be made for decisions below the Manage Risk drop down box (image 9.7). This is done to keep record for later parties why the decision was made.

CONTROLS TAB

In the Controls Tab for an individual Threat the system will suggest controls that work against the risk in question. The assessor must go through the list and set the Status (image 9.8) for each one.

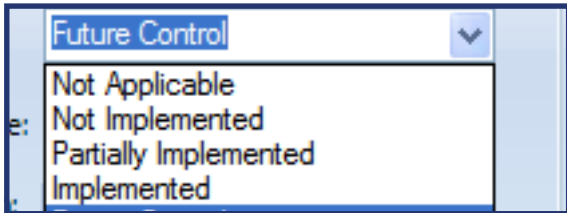


Image 9.8- Status

A list of all Standard controls from ISO/IEC STANDARD (or the User Defined Standard) appears in a list on the screen.

There are e.g. 133 Standard controls for ISO/IEC 27001. All the controls must be reviewed and a status assigned to them.

- Implemented
- Not implemented
- Partially implemented
- Not applicable
- Future Control

Note that a control can be partially implemented. This is when a security control has been implemented but not to its full extent. An example of this would be, e.g. if plans for business continuity were well on their way but were not fully complete.

Keep in mind that a Standard control recommended by the system may be inapplicable in some cases. An example of such an instance would be a business without a computer system. If this were the case, there would be various inapplicable Standard controls. Enter information that supports the Assessment under Justification.

You can add controls by clicking on the Add New Control Icon in the Controls Toolbar above the Controls List.

Make sure that all the Standard controls have been reviewed before going on to the next tab in the Risk Treatment.

SCHEDULING A FUTURE CONTROL

When scheduling a future control you should enter information in the Justification text box, on why you categorize a Control as a Future Control.

You will then formally schedule the future control in the next tab, Future Controls.

FUTURE CONTROLS TAB

The last tab in the Risk Management Tab is Future Controls. In this tab all the Future Controls for a given Risk, selected in the Risk Management List, are displayed.

Here you should schedule when you plan on implementing the given Control.

OVERVIEW

The last two tabs on the individual Risk Treatment Pane are Overview tabs. Here you can see an Overview of all the Controls as well as all the Future Controls pertaining to the given Risk Treatment. You can conveniently modify the columns according to your needs (image 9.9).



Image 9.9 - Overview

RELOAD ASSETS, THREATS AND CONTROLS

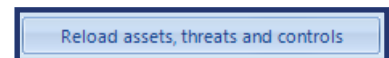


Image 9.10 Reload button

In RM Studio® we offer the user the possibility to manually control reloading of assets, threats and controls when working in Risk Treatments (image 9.10). Before version 2.3 the Risk Treatment got updated when the associated Risk Assessment or the mitigating control library got updated. This reload therefor happened automatically upon save. With version 2.3 the option has been added to the user to i.e. delete controls from the Risk Treatment, that is to change the threat-control associations in the Risk Treatment level to be more aligned to the user need. This means that the user can now i.e. delete controls from either an asset level (from the Management Tab – grouped by an asset) or from global level (from the Controls Tab).

The function of this button is as follows:

- I. If the list of assets has changed in the Risk Assessment, the new assets and

their associated threats from the Risk Assessment get reloaded.

2. If the list of threats associated to a particular asset has changed in the Risk Assessment the risks are reloaded into the Risk Treatment.
3. If the mitigating controls to risks in the Risk Assessment have changed those controls get reloaded into the Risk Treatment as mitigating controls to that risk.
4. If a new control has been added to the Gap or Standard used when creating the Risk Treatment, these new controls are loaded into the Risk Treatment.
5. In general the list of controls is reloaded, based on the threat-control library as well as the Standard/Gap that was used.

RIGHT -CLICKING

Users can now manage multiple treatment options by selecting those Threats and right-click on the selection. The options provided to the user is to change the name of Threat treatment(image 9.11)

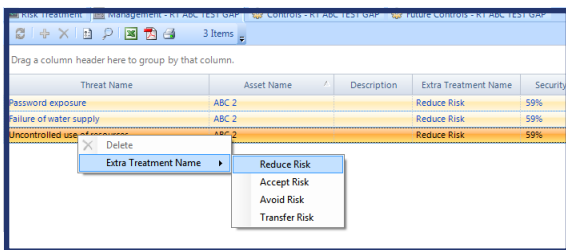


Image 9.11 - Right Clicking

13. DEFINITIONS

DEFINITION OF ASSET EVALUATION VALUES

RM Studio® comes with a Standard definition of asset and threat properties. These definitions can be changed via the Evaluation Templates. The Standard definitions are as follows:

INTEGRITY

Low

It is not important that the asset is accurate.

Medium

It is important that the basics are accurate.

High

The asset has to be reasonably accurate.

Very High

The asset must be complete and accurate, but details (e.g. appearance) are irrelevant.

Immense

The asset must be complete and accurate.

AVAILABILITY

Low

The asset is not necessary for operating the business entity.

Medium

It is possible to operate the business entity without the asset. It has to be available again in 24 hours.

High

If the asset is not available it is difficult but possible to proceed working for 2-3 hours.

Very High

The asset has to be available during working hours.

Immense

The asset has to be available 24 hours a day.

VALUE

Low

Easy and inexpensive to regain the asset.

Medium
Possible to operate business entity for a time period if loss of asset occurs.

High

Difficult to continue operation without the asset. Difficult to regain the asset if loss occurs.

Very High

Very difficult to continue operation without the asset. Very difficult to regain the asset if loss occurs.

Immense

Not possible to operate the business entity without the asset. Immensely difficult to regain the asset if loss occurs.

CONFIDENTIALITY

Low

Public may be aware of the asset. It may be discussed and published.

Medium

Employees have access to or are aware of the asset. Information must be treated with caution towards third party.

High

Most employees are aware of or have access to the asset. Intended for use inside the business entity only. Must not be disclosed to third party.

Very High

Key employees are familiar with the asset but many employees are aware of it.

Immense

Only key employees have access to and are aware of the asset.

DEFINITION OF THREAT EVALUATION VALUES

VULNERABILITY OF ASSET

Low

Despite of the occurrence of the threat, the asset will be unchanged.

Medium

If the threat happens the asset might be damaged or be unusable to some extent.

High

If the threat happens the asset might be damaged or be unusable.

Very High

If the threat happens the asset will be damaged to a great extent.

Immense

If the threat happens the asset will cease to exist or be unusable.

Low

The threat is likely to happen less than once a year.

Medium

The threat is likely to happen once a year.

High

The threat is likely to happen once a month.

Very High

The threat is likely to happen once a week.

Immense

The threat is likely to happen once a day.

IMPACT OF THREAT

Low

Minimal impact of threat

Medium

There is some impact of the threat.

High

Much disturbance in operation. Considerable time and investment required to go back to normal operation.

Very High

Serious disturbance in nearly every part of the operation. Much time and investment to go back to normal operation.

Immense

The consequences of threat are widespread and cause serious disturbance in operation. Very difficult to go back to normal operation.

14. GLOSSARY

ASSESSMENT

An Assessment is the act of evaluating something. Here it means that the organization is evaluated in comparison to Threats that are aimed at its Assets, i.e. Risk.

ASSET

An Asset is anything of value to the organization.

AVAILABILITY

How readily obtainable or accessible a given asset is.

BASE SECURITY RISK

The calculated Risk that a organization faces based on the probability of each threat occurring, the impact it would have on the organization, the organization's vulnerability towards the threat, and the value of the Assets affected by each threat to the company.

BASIC CRITERIA

A statement of what Risk the organization is willing to accept.

BUSINESS ENTITY

Your organization or part thereof. Business Entities can also be many other things, e.g. a different company or a client.

CATEGORIES

Categories are any general or comprehensive division. Here specifically it is the division of Assets according to the applicable Standard.

CODE OF PRACTICE

A code of practice is an guide on best practices to implement a Standard.

CONFIDENTIALITY

The principle that all information regarding a particular Information Asset needs to be held secret, unless the organization gives consent permitting disclosure.

CONTROLS

A Control is a set of procedures in a particular Standard that once applied act to control, regulate, and hedge against known Threats.

CURRENT SECURITY RISK

Security risk with regards to implemented controls. Each single Threat in the system is related to a number of Controls from the Standard, which hedge against it. The Current Security Risk is calculated with regards to that so the more Controls that are implemented the lower the Current Security Risk is.

FOUR DIMENSIONAL MATRIX

A graphic representation of our Risk calculations. The Significance of a Threat is juxtaposed with the Probability of the Threat. Likewise the Vulnerability of the Asset is juxtaposed with its Value. The resulting value of the conjugated values is then used in the Risk Calculations.

GAP ANALYSIS

Gap Analysis is an assessment tool enabling the user to compare their actual state in regards to a particular Standard with what is needed to be eligible for certification.

IEC

International Electrotechnical Commission. An international Standards organization dealing with electrical, electronic and related technologies.

IMPACT

The effect that it will have on the organization should a given Threat occur.

INFORMATION PANE

A part of the graphical user interface that displays information on a given subject. Here particularly it refers to the lower half of the screen where, when an item is selected in a list above, usually a pane will appear with information on that item.

INFORMATION SECURITY

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

INTEGRITY

How important it is for the organization that the Information Assets are complete and accurate.

ISO

The International Organization for Standardization (Organization internationale de normalization), is an international-Standard-setting body composed of representatives from various national Standards organizations.

ISO 9001

Is an international Standard for quality management systems. It provides a number of requirements which an organization needs to fulfil if it is to achieve customer satisfaction through consistent products and services which meet customer expectations.

ISO/IEC 14001

ISO 14001 is the international specification for an environmental management

system (EMS). It specifies requirements for establishing an environmental policy, determining environmental aspects and impacts of products/activities/services, planning environmental objectives and measurable targets, implementation and operation of programs to meet objectives and targets, checking and corrective action, and management review.

ISO/IEC 27001

Is an information security management system (ISMS) Standard published in October 2005.

ISO/IEC 27002

The Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls.

MENU BAR

Also known as the Ribbon. It is the top most part of the application where the most common functions are placed for your convenience.

NAVIGATION TREE

A navigational tool that allows the user to expand and collapse items representing parts of the software that have been divided into nodes simulating a tree with branches. This allows users to access nested nodes with ease.

PROBABILITY

The likelihood of the Threat occurring.

PROCESS

A systematic series of actions directed to some end. Here specifically it is the name of the node in the Navigation Tree that groups the Assessments, Gap Analysis and Risk Treatment processes together.

REPORTING SERVICES

A server-based report generation software system from Microsoft. It can be used to

prepare and deliver a variety of interactive and printed reports.

REPORT

An account or statement describing in detail an event, situation, or the like, usually as the result of observation, inquiry, etc.

RISK

The relationship between a Threat and an Asset is defined as Risk.

RISK ASSESSMENT

Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat.

RISK MANAGEMENT

Risk management is activity directed towards the assessing, mitigating (to an acceptable level) and monitoring of risks. In some cases the acceptable risk may be near zero. Risks can come from accidents, natural causes and disasters as well as deliberate attacks from an adversary.

RISK TREATMENT

Once Risks have been identified and assessed, all techniques to manage the Risk can be defined as Risk Treatments.

SCOPE

Scope defines the extent or range of the Risk Assessment. That is, which parts of the organization will be taken into account during the Assessment.

Standard

A technical Standard is an established norm or requirement. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices.

STATEMENT OF APPLICABILITY

Is a document which identifies the controls

chosen for your environment, and explains how and why they are appropriate.

THREATS

An indication of impending danger or harm. Here specifically towards Information Assets. A Threat is anything that jeopardizes the Confidentiality, Integrity, Availability or Value of the Asset.

VALUE

Value is the relative worth, merit, or importance of an object. Here specifically it is the qualified worth of an Information Asset.

VULNERABILITY

Defines how vulnerable an Information Asset is towards a threat.

15. CONTEXT & FLOW

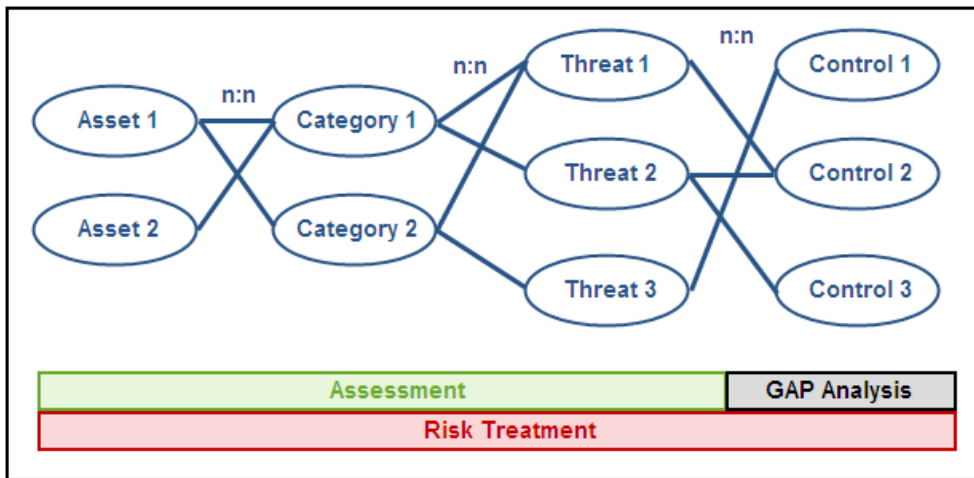


Image 15.1 - Context

CONTEXT

Figure 15.1 shows abstract diagram of the relationship between the Assets, Categories, Threats and Controls. Additionally the figure shows the scope of each of the three core processes in relation to the aforementioned entities. It should be noted that the relationship on every level is n:n meaning that every asset can have many categories, but every category can be in more than one asset. One consequence of the repeated n:n relationships demonstrated in the figure is that, should a table list all possible connections then it would have several thousand lines. This is one of the reason why in the management tab of the risk treatment window the aforementioned information is represented in two tables.

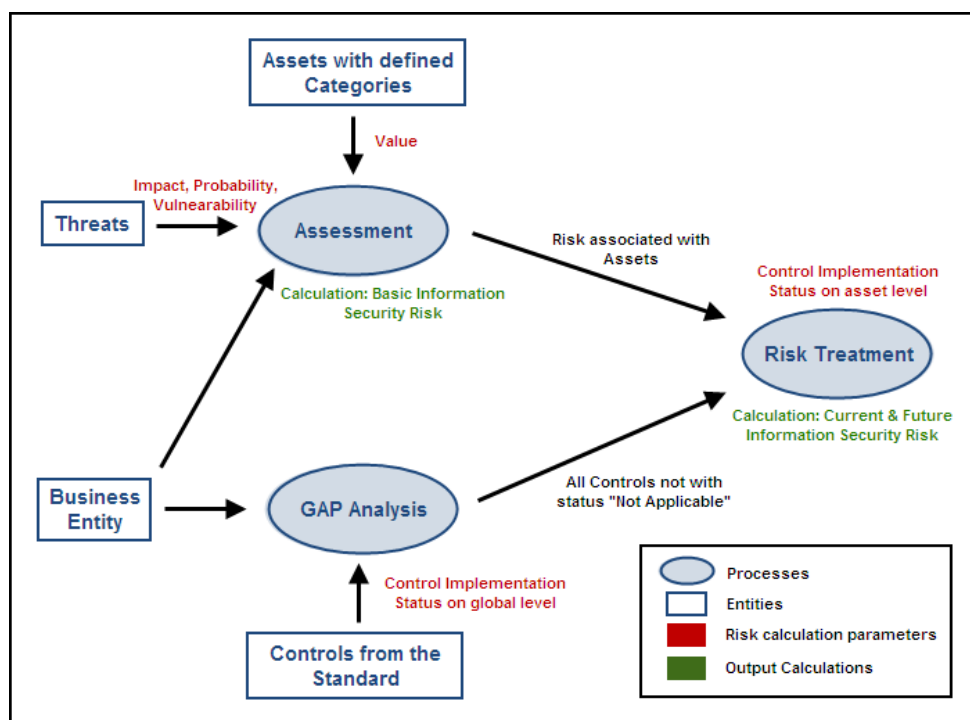


Image 15.2 - Flow

FLOW

Figure 15.2 Shows an abstract diagram of the relationship between the three core processes and entities of RM Studio®. It can be clearly seen that the Risk Treatment uses information from both the Assessment and the GAP Analysis (which is optional). It should also be noted that the GAP Analysis; is independent from the Assessment , and it has no association with the Threats nor the Assets and is therefore a global Process.

16. CALCULATIONS

In these examples the calculations are based on the Standard Evaluation Templates. Calculations for user defined Templates are slightly different.

SECURITY RISK

The security risk is a factor calculated from the values set for the asset value, significance of threat, probability of threat and vulnerability of assets. The security risk ranges between 0% (minimum) and 100% (maximum), where the range is divided into percentages. The security risk can be reduced by implementing the controls suggested by RM Studio®. When all the controls suggested by RM Studio® have been implemented, the security risk is reduced to MIN.

The different values for the security threats are calculated as follows:

1. FIRST RISK CALCULATION

The first security risk calculation which is also known as the base security risk starts with a single risk and is based on four variables, the probability of the risk, the impact of the risk, the vulnerability of the asset towards the risk and the value of the asset of which the threat risk is associated with. All of these four variables have been evaluated on the scale between 1 and 5. What we do is we add all the four evaluations together and divide with the highest possible number, that is 20, but we also shift the result by 3 to the left. So we end up having:

$(\text{Probability} + \text{Impact} + \text{vulnerability} + \text{value} - 3) / (20 - 3)$.

The results for various values of these variables can be seen in the four dimensional matrix at the end of the user manual.

2. SECOND RISK CALCULATION

The second risk calculation is called current security risk or security risk with regards to implemented controls. Each single threat in the system is related to a number of controls from the Standard, which hedge against it. So, for example if we have a threat which was evaluated immense for all the four variables, that particular risk would have the security risk of 100% or Maximum security risk. In this example let's say that this particular threat is related to 10 controls from the Standard, and let's say that 8 out of those ten controls have been implemented. We multiply the security risk with the ratio of controls which have not been implemented which in this case is 2/10 so the security risk with regards to implemented controls will go down from 100% to 20%.

3. THIRD RISK CALCULATION

The third risk calculation is similar to the second risk calculation. It takes into consideration both implemented and future controls while the second risk calculation only takes into consideration implemented controls. If we stick to the example given for the second risk calculation, let's say that the remaining two controls will be scheduled to be implemented in a couple of months and will be changed into future controls. If we now calculate the security risk with regards to implemented and future controls we will multiply the security risk with the ratio of controls which have not been implemented and have not been defined as future controls. In this example the security risk with regards to implemented and future controls will be 0% or Minimum.

4. SECURITY RISK OF AN ASSET AND THE RISK ASSESSMENT

The Risk calculations start with a single Risk and is calculated for every Risk in the Risk Assessment. An Asset also has a Security Risk. The Security Risk of an Asset is simply the average of all the Security Risks which are associated with that particular Asset. The Risk Assessment also has a Security Risk, this Security Risk is calculated by getting the average of the Security Risks of all the Assets in the Assessment.

to the Threat it is under. This matrix is a supplement to the risk calculation section covered previously in this manual.

RESIDUAL RISK

Below is the matrix used for establishing the security risk of an Asset in relation

		Probability of Threat					Significance of Threat																				
		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5						
Asset Value	Vulnerability of Asset	1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9
		2	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10
		3	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
		4	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12
		5	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13
1	1	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	
	2	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	
	3	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	
	4	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	
	5	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	
2	1	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	
	2	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	
	3	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	
	4	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	
	5	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	
3	1	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	
	2	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	
	3	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	
	4	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	
	5	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	12	13	14	15	16	
4	1	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	
	2	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	
	3	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	
	4	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	12	13	14	15	16	
	5	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	12	13	14	15	16	13	14	15	16	17	
5	1	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	
	2	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	
	3	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	12	13	14	15	16	
	4	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15	12	13	14	15	16	13	14	15	16	17	
	5	10	11	12	13	14	11	12	13	14	15	12	13	14	15	16	13	14	15	16	17	14	15	16	17	18	

It's important to realize that when using the security risk calculation with regards to controls, it is possible to get the security risk down to 0%. What this means is that you have done everything you possibly can to minimize the security risk "with regards to the Standard". You have implemented all the controls which are associated with the threats you have defined in your risk assessment. Therefore the risk calculation tells you that you have 0% or minimum security risk. Please keep in mind that this does not mean that you do not have security risk but it only means that you have done everything in your power, based on the Standard, to hedge against known threats.

17. CREDITS

ICONS IN RM STUDIO

The icons used for the RM Studio® software are Pinvoke icons.

<http://www.pinvoke.com/>

FRONT PAGE

The image used is obtained from www.sxc.hu

COPYRIGHT

ISO Standards that are reproduced in this software are with the permission of the International Organization for Standardization, ISO.

No part of these Standards may be reproduced in any form without the prior written consent of ISO at copyright@iso.org. ISO Standards can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at www.iso.org. Copyright remains with ISO.

RISK MANAGEMENT STUDIO MANUAL



Stiki ehf. - Information Security

Laugavegur 176 - IS-105 Reykjavik, Iceland

Tel: +354 5 700 600 - Fax: +354 5 700 601

www.stiki.eu - stiki@stiki.eu



Membership No. 140



Certificate No. IS 67387
ISO 27001



Certificate No. FS 67386
ISO 9001