

SecureAware®

SecureAware Risk Manual

Applies to SecureAware version 3

Document date: April 2009

Table of content

SecureAware Risk.....	3
Installation	3
Technical data	3
License key installation.....	3
How to begin a Risk Assessment.....	4
Systems	5
Processes	6
Assets	7
Executing a risk assessment	8
Business Impact Assessments	9
Vulnerability Assessments	9
How the risk calculations are performed.....	10
Contact Information	12

SecureAware Risk

SecureAware Risk is Neuparts standard solution for Information Security Risk Management.

Installation

SecureAware Risk is to be installed at a server in the customer's infrastructure. Users access the SecureAware solution using a browser.

After running the setup program, you'll need to start the SecureAware 3 Server Service. This can be done from either Windows service manager or from SecureAware Service Manager. The setup program launches the latter.

Technical data

Operating systems

Windows 2000, Windows 2003, Windows XP, Linux Red Hat 7 and higher are supported.

Browser compatibility

Microsoft Internet Explorer 6.0 and Firefox 1.0, or higher.

Server capacity

Free memory for SecureAware at server at least 256MB; 512MB recommended.

Disk space: At least 300MB free; 600MB recommended.

License key installation

- Point browser to `http://<servername>:8080/`
- Login as user 'sa' with password 'snRt!32w'
- Click the license icon , choose portal SecureAware, point to license key file and click 'Upload'
- Logout

How to begin a Risk Assessment

Login as Super User ('su')

- Point browser to `http://<servername>:8080/`
- Login as user 'su' with password 'snRt!32w'

Create Internal Uses

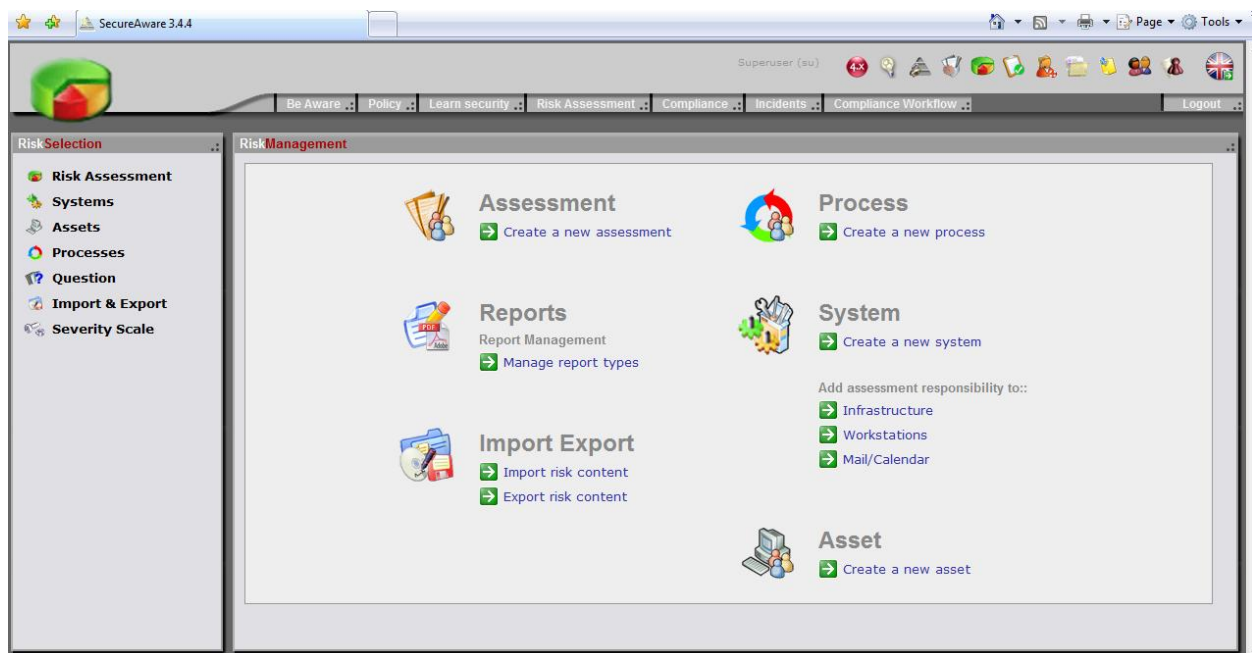
In the following we will assume that SecureAware Risk is configured to use internally defined users.

- Choose the User Management icon
- Create the users you will need to start your first assessment. This will typically be a technical IT infrastructure or application platform person and a manager.

Super User's Main Page for Risk Assessments

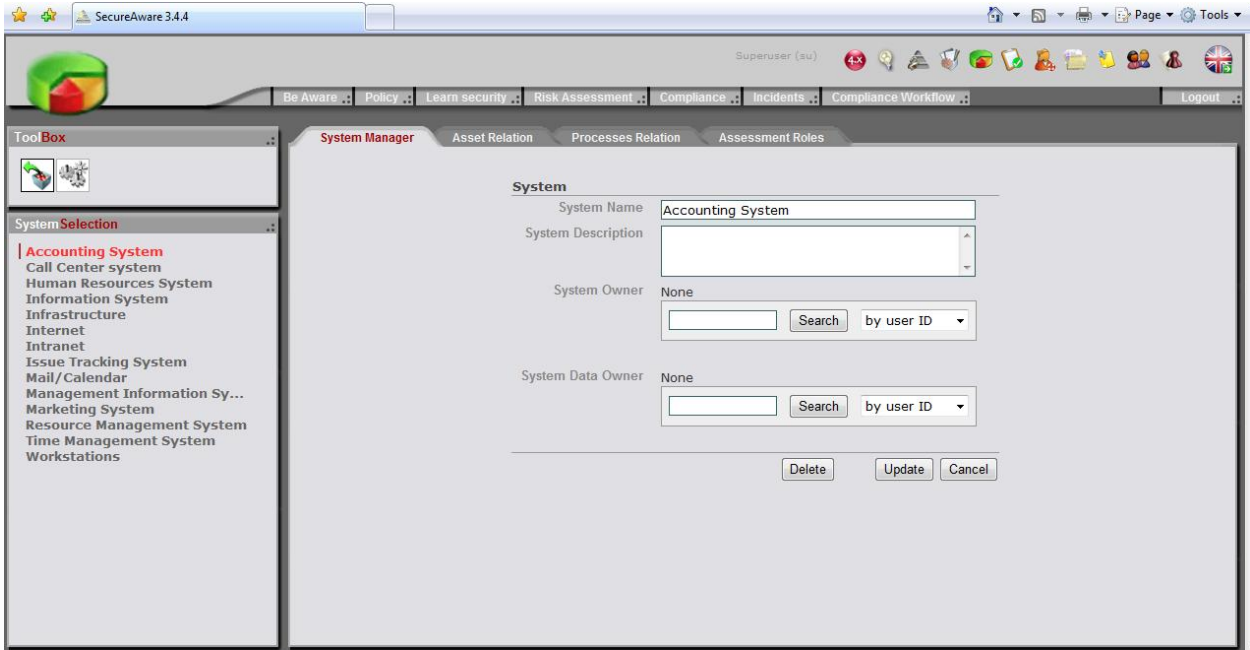
You'll find the main page by selecting the Risk Icon topmost on the screen or by clicking **Shortcuts** on My SecureAware (the start page) and selecting the Risk shortcut.

- If you are a super user, you will often need this.



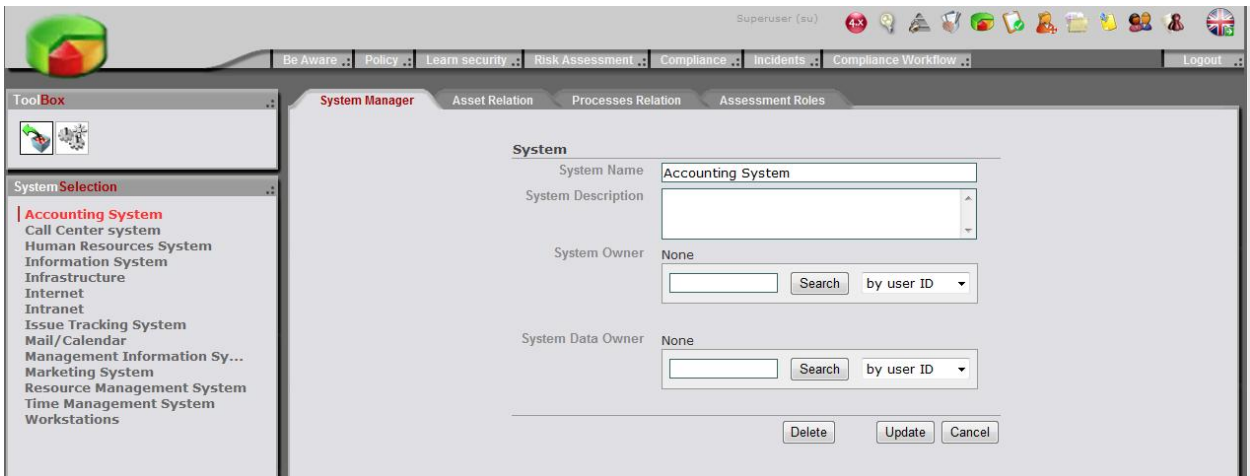
Systems

Before you can assess risks, you will need specify who will be responsible for assessing business impact and vulnerabilities. Super user specifies this in Systems Settings in the tab named 'Assessment Roles'



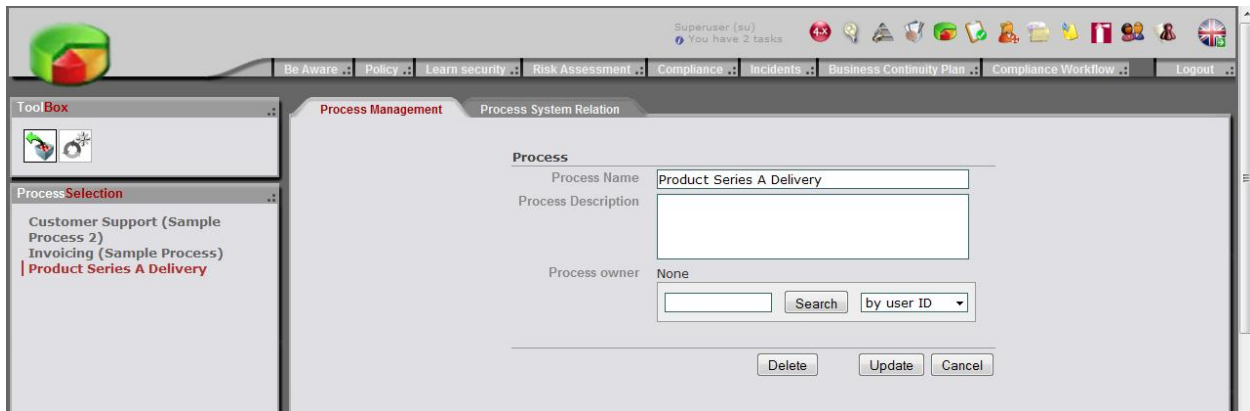
Create and Start an Assessment


Go back to super user main page and choose "Create a new assessment". Assign a name. E.g. Assessment2006. Then go to main page and select "Start Assessment2006". Then click the start button. Log out.




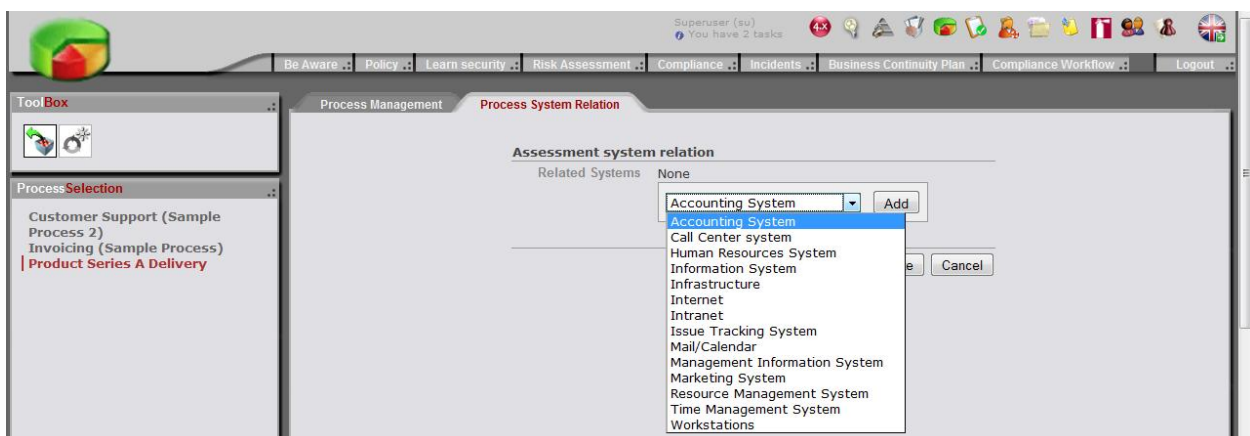
Processes


To gain a more detailed overview of the risk factors facing your company, you can attach specific risk-assessment processes to your various systems.



Click on  **New process** in the main menu. You will now be presented with some example processes.


By clicking on  under ToolBox at the top left of the screen, you will be able to create a new process from scratch. Once you have given your new process a name and a description, you can designate a process owner by searching user IDs, names or emails. Once selected, click **Update** to save your changes.

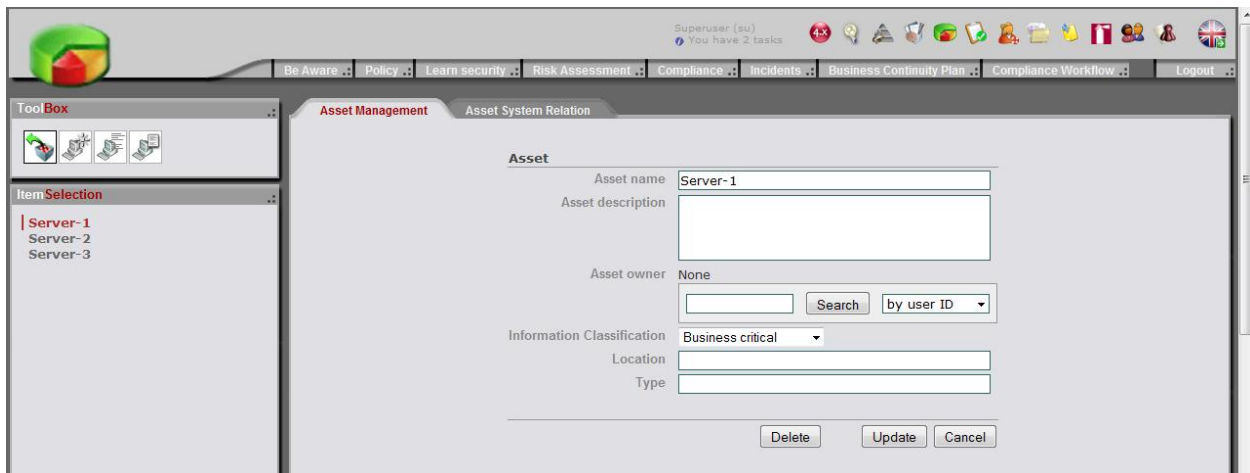


You can now link the process to a specific system. To do this, mark the process in the Process Selection menu on the left and select the **Process System Relation** tab. Now, select a system from the drop-down menu and (once selected) click on **Add**. Repeat as necessary if you want to add more systems. To remove a system, click on  beside the system name. Finally, click **Update** to save or **Cancel** to undo.

Assets

Just as certain risk-assessment processes can be linked to specific systems, risk-assessment processes can also be linked to specific assets. Assets are components of your IT infrastructure used by a system to manage system information, including servers, communication infrastructure and programs.

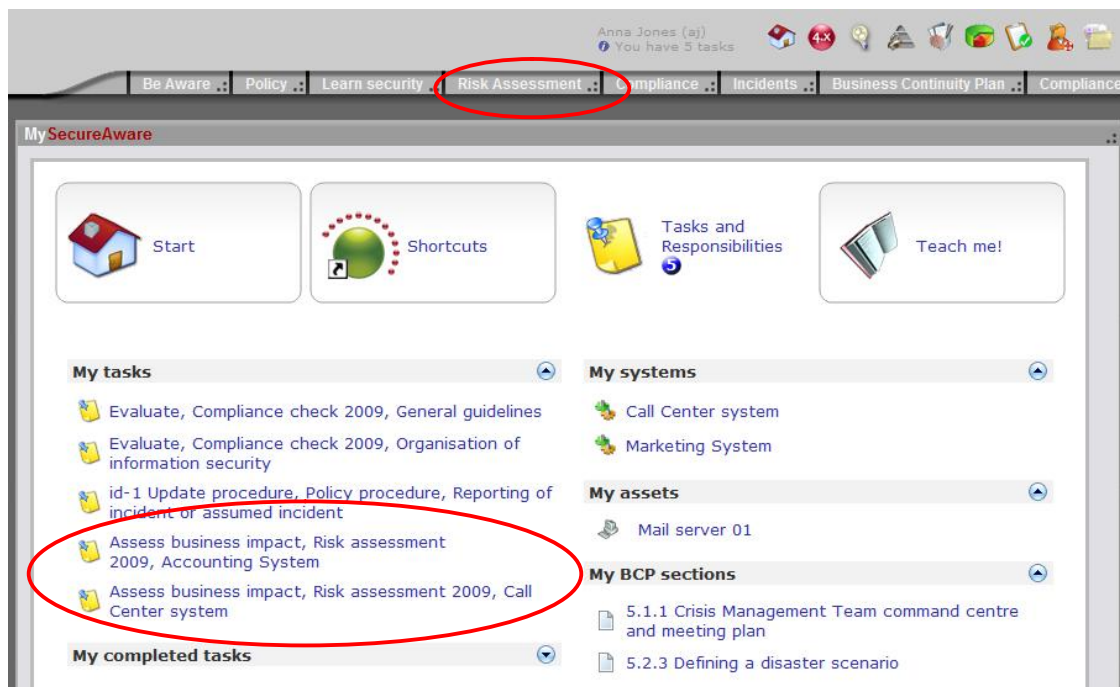
Click on  **New asset** in the main menu to access the Assets menu. In the same way as with processes, once you have named and provided a description for your asset you can create an asset an owner by searching IDs, names or emails and also determine whether your asset should be linked to one or more systems. Remember to click **Update** to save or **Cancel** to undo.



The screenshot shows the SecureAware web interface for Asset Management. The main menu at the top includes: Be Aware, Policy, Learn security, Risk Assessment, Compliance, Incidents, Business Continuity Plan, Compliance Workflow, and Logout. The user is logged in as Superuser (su) and has 2 tasks. The interface is divided into a left sidebar and a main content area. The sidebar contains a 'Tool Box' with icons for various actions and an 'Item Selection' list with 'Server-1', 'Server-2', and 'Server-3'. The main content area is titled 'Asset Management' and 'Asset System Relation'. It features a form for creating or editing an asset with the following fields: 'Asset name' (text input with 'Server-1'), 'Asset description' (text area), 'Asset owner' (set to 'None' with a search button and a dropdown for 'by user ID'), 'Information Classification' (dropdown menu set to 'Business critical'), 'Location' (text input), and 'Type' (text input). At the bottom of the form are three buttons: 'Delete', 'Update', and 'Cancel'.

Executing a risk assessment

Your personal risk assessment tasks will be shown on My SecureAware under the **Tasks and responsibilities** tab. Click on a task to commence your assessment. Alternatively, click on the **Risk Assessment** tab. You now have two options: read an introduction to your assessments, or start assessing the vulnerability of the systems for which you are responsible and evaluate the Business Impact should these be compromised.



How the risk calculations are performed



Risk is calculated as the likelihood for an incident multiplied with the business impact of such an incident:

$$\text{Risk} = \text{likelihood} * \text{business impact}$$

The likelihood of an incident depends on the vulnerability of a system, combined with the amount of interest in impacting the system.

Vulnerability depends on threats and mitigating controls. In SecureAware Risk, vulnerability can be assessed or analyzed in two ways:

1. Quick and simple: The person responsible for assessing vulnerability chooses the level of vulnerability from a pre-defined scale. (E.g. 1-5)
2. More detailed: The person responsible for the assessment answers a questionnaire, where the input is used to assess the level of vulnerability.

To list every possible threat against each system is practically impossible. It is much more operational to evaluate the different threats when assessing mitigating controls.

This is why SecureAware Risk contains a questionnaire, which can be used to assess the vulnerability of each system, based on which mitigating controls are in place to reduce the threats to the system in question. If the questions are answered in a way that gives the highest level of points, it means

that mitigating controls against each threat is implemented, and there is full compliance with best practices for it-governance. In that case the vulnerability for this system will become the lowest possible.

If the answers, on the other hand, give the lowest level of points, then the system vulnerability will become the highest possible.

The points from the questionnaire answers are transformed into a vulnerability score, based on vulnerability assessment scale used by the assessment. As Superuser, you can adjust this conversion scale individually for confidentiality, integrity and availability. You find this in the Settings menu in SecureAware Risk.

The vulnerability score is combined with interest factor to calculate the likelihood level. It is this likelihood that is reported in the risk report . The calculation of likelihood is conducted using a pre-defined table. This table is adjusted in the settings menu as well. By default, the calculation is based on a 1-5 scale, which functions in this way:

- If the level of interest is "medium", the likelihood equals the level of vulnerability.
- If the level of interest is more than "medium", then the likelihood of an incident rises.
- If the level of interest is less than "medium", then the likelihood of an incident is reduced.

The principle of conversion can also be explained in the way that even though a systems technical vulnerability is "very low", then the likelihood of an incident will be more than "very low" if the level of interest to break into that system is high.

If a system, on the other hand, isn't interesting, then the likelihood of an incident will decrease, despite of the level of vulnerability. Likelihood will certainly not drop to zero, but it will be reduced compared to a more interesting system.

The calculation of the level of likelihood can also be adjusted by a Super user.

Contact Information

- Further information is available by contacting Neupart

Europe

Neupart A/S
Hollandsvej 12
2800 Lyngby
Denmark
Tel +45 7025 8030
Fax +45 7025 8031

North America

United States
Neupart Inc.
2553 Crescent St
Ferndale, WA 98248
Tel. 360-820-2545
Fax 360-392-6078

Neupart GmbH
Kaiserwerther Strasse 115
40880 Ratingen/Düsseldorf
Germany:
Tel. +49 (0) 2102/4209-26
Fax +49 (0) 2102/42062

Copyright © 2006 Neupart A/S. All rights reserved.

The author of this documentation is Neupart A/S. All information herein including text and graphics belongs to Neupart A/S unless stated otherwise and is protected by copyright laws in Denmark and international agreements.

Permission to quote this documentation in its entire form or partly is given under the premises that no changes are made and that information about this copyright is clearly stated on all copies. No material may be copied or distributed without explicit approval of Neupart A/S. Neupart A/S preserves the right to - at any time and without warning - make changes and/or improvements in the products mentioned.

Names of other companies and their products are or can be registered trademarks or trademarks that belong to their owners. Neupart and SecureAware logo and the name "SecureAware" are trademarks belonging to Neupart A/S.

The documentation is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the documentation or the use or other dealings in the documentation. The documentation including graphics could contain inaccuracies or typographic errors. Furthermore there are no guarantees regarding results achieved by using this information.

All rights not explicitly mentioned herein are preserved.