



User Guide



Document reference: NSC-649-039 Issue: 2.4 1 April 2010

Quantar Solutions Ltd. • Cambridge • United Kingdom • www.quantarllp.com

Newman & Spurr Consultancy Ltd • Camberley • United Kingdom • www.nsc.co.uk

This document was written by Newman & Spurr Consultancy Ltd (NSC) for Quantar Solutions Ltd.
Copyright © Quantar Solutions Ltd. 2010.

1	INTRODUCTION.....	1
1.1	n-ORM.....	1
1.2	Data Flow	1
1.3	Terminology	1
2	GETTING STARTED	3
2.1	Installing n-ORM	3
2.2	Creating a Portfolio and Baseline Scenario	3
2.3	Navigation	3
2.4	Summary Pages.....	3
2.5	Configuration.....	4
3	ACTIVITY PREDICTION.....	5
3.1	Purpose.....	5
3.2	Viruses and Hacks	5
3.3	Physical Attacks	5
3.4	Output	5
4	VALUE AT RISK.....	7
4.1	Purpose.....	7
4.2	Define Infrastructure.....	7
4.3	Variance from Baseline	8
4.4	Reports.....	8
5	WORKING ACROSS MULTIPLE SITES.....	9
5.1	Delegated Infrastructure.....	9
5.2	Aggregated VAR	9
6	OTHER TASKS	11
6.1	Audit History.....	11
6.2	Non-interactive Mode	11
7	GLOSSARY	13

1 Introduction

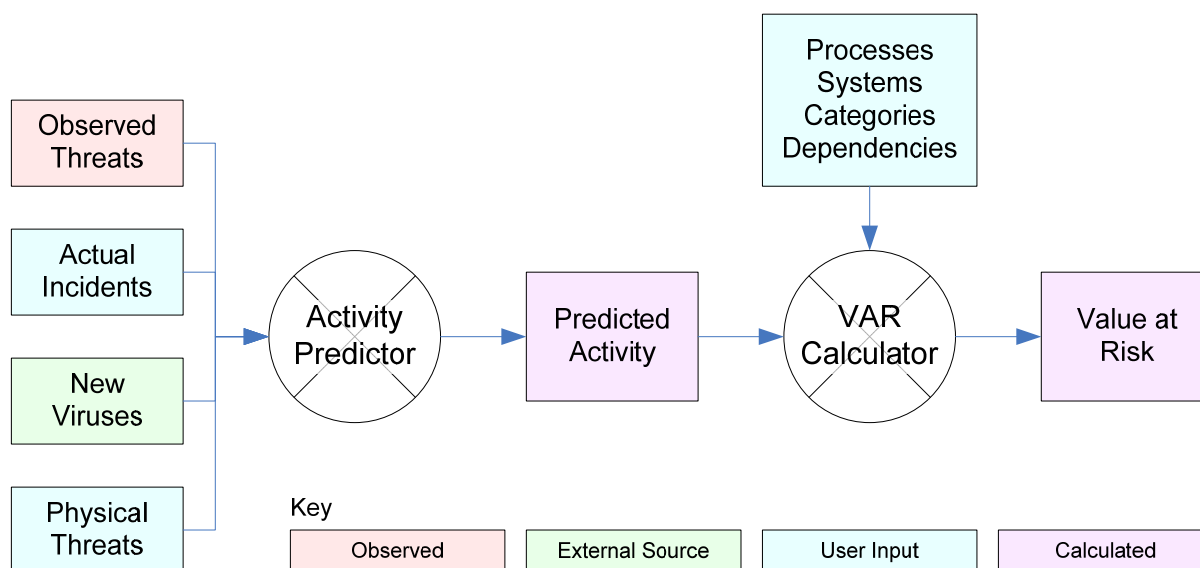
1.1 n-ORM

n-ORM™ is a tool to measure and manage your risk associated with attacks to your enterprise IT infrastructure. Threats to the network arise in various forms, such as viruses, hacking attempts and physical attacks. n-ORM monitors network traffic outside the corporate firewall over time and uses sophisticated algorithms to predict likely threat levels in the next time period. Once you have defined your infrastructure with the easy-to-use graphical tool provided, n-ORM calculates your value at risk from those threats.

You can analyse the composition of the risk by business process or company division. Using a portfolio containing multiple scenarios allows you to determine the effect of changing your infrastructure on the risk burden.

1.2 Data Flow

A high-level overview of the algorithms in n-ORM and their inputs and outputs is shown in the diagram below:



The observed data (pink) is obtained from analysis of network traffic sampled from outside the firewall. All user input (blue) is entered via n-ORM's graphical interface. Counts of new viruses in the wild (green) are sourced over the internet. The data and calculations are described in more detail later on, in sections 3 (Activity Prediction) and 4 (Value at Risk).

1.3 Terminology

Some terms used in this document have a particular meaning to n-ORM. The first time each is used, it is highlighted **thus**. They are defined in the glossary at section 7.

2 Getting started

2.1 Installing n-ORM

n-ORM may be installed on Windows (2000 or later) or Linux (kernel version at least 2.6). Both 32-bit and 64-bit versions are provided for each operating system. Full installation instructions are provided in the InstallGuide.txt file in the top-level folder on the CD.

Before running n-ORM, ensure that a licensing dongle is inserted into a USB port on your PC. Without a dongle being present, n-ORM will run in a limited-functionality trial mode which restricts the size of the infrastructure that can be modelled. The dongle must remain present while the program is running.

2.2 Creating a Portfolio and Baseline Scenario

The first time that n-ORM is started, you must create a new **portfolio** file in which to contain **scenarios** that store the **physical threats** and **infrastructure** data. Choose a location and filename (a “.npf” extension will be supplied automatically) and click Create. The baseline scenario is automatically created in the new portfolio. On subsequent occasions, you can choose an existing portfolio from the list or create a new one.

2.3 Navigation

The bar at the top of every page has buttons at the sides and tabs in the middle. The buttons control the active page and navigation within n-ORM, including Back, Accept Changes, Print, Configuration and About. Hover the mouse over any button for a brief description. The tabs are used to switch between open scenarios in a portfolio and to display the page title. Click a tab to switch to that scenario; click the cross on a tab to close it. You cannot close the first (portfolio) tab.

2.4 Summary Pages

Once the portfolio is created, you are taken to the main Portfolio Summary page. This shows you a table and chart of the scenarios in the portfolio and the value at risk in each. Beneath the table is a summary of the electronic threats to the network. These are calculated from observations and historical data, so are shared between all scenarios. Use the Edit button at the bottom to show observations and projections page. This has a table of threat data of attempted and successful attacks. Attempted attacks are obtained from the network traffic inspection part of n-ORM; you must enter successful attacks on this page. Information about new **viruses** appearing in the wild is obtained automatically over the internet as it is published monthly.

Back on the Portfolio page, the buttons above the table allow you to create or open another portfolio and to manage the scenarios in the currently open portfolio. Selecting a scenario in the table then clicking the Open Scenario button displays the Status Summary page. This serves as a hub for the scenario. You can edit the scenario name and implementation cost (except for the Baseline

scenario) and view summaries of the threat data, infrastructure and value at risk. There are buttons to move to other pages to input data and access output reports.

2.5 Configuration

You can configure n-ORM in various ways to suit your enterprise. The configuration page is accessed from a button on the toolbar. Options include:

- a. Where certain files are stored. Apart from the scenario file, n-ORM uses various other files to store attempted and successful attack data and audit data. They may be located in any directory that you have permission to access, including network fileshares.
- b. The name of the **location** where this instance of n-ORM is deployed (see section 5.2 Aggregated VAR for how this is used).
- c. How far back to look at historical data when predicting future activity.
- d. How to display financial data: the currency symbol and scale factor. The currency symbol (e.g. \$, £, €, USD) is purely for display purposes – n-ORM does not do any currency conversions. If you change the symbol from \$ to £, the numbers output remain the same (what was displayed as \$1,000K is then shown as £1,000K). The scale factor is accounted for in the calculations: changing from Thousand to Million means what was displayed as \$1,000K is then shown as \$1M.
- e. A weighting factor to apply to the value of **processes** marked as outsourced.
- f. The language used for the user interface. n-ORM is supplied in English and several other languages. Where available, it uses the language your operating system is set to use. If you prefer a different language, select it on this page.

3 Activity Prediction

3.1 Purpose

The activity prediction engine in n-ORM is used to calculate the expected number of **attacks** on each part of the IT **infrastructure**. It is run in the background each time the input data is changed to ensure the output is always kept up to date.

3.2 Viruses and Hacks

On the summary page, you must enter the number of **viruses** and **hacks** that penetrated your corporate firewall for each period shown by typing into the table. (See the glossary for the definitions of those terms used by n-ORM.)

These numbers are compared to an analysis of the network traffic sampled from outside the firewall and the number of new viruses identified worldwide for the same periods. Trends in the comparison are extrapolated to give the predicted number of viruses and hacks for the next period.

3.3 Physical Attacks

Physical Threat data must be entered manually based on a risk assessment of the enterprise IT system. Possible threats include fire, theft, terrorism or loss of power. The data is entered on the Physical Threats page accessed from the Summary page.

You may enter as many threats as you wish. Each threat may be given a name to identify it. It must have a target, which should match a **System Category** defined in your infrastructure (see the Value at Risk section below). The severity of the threat reflects the level of damage it would cause to Systems should the threat materialise; it is an arbitrary scale from 1 to 10, corresponding to the vulnerability defined for System Categories (see later). You should also define the assessed frequency of incidents, e.g. one per month or two per decade.

If you wish, you may define a time profile for each threat. This allows a more accurate calculation of the value at risk to certain processes. For example, a power cut on a Saturday may have a lesser impact than on a Monday morning. You define the profile by setting the relative frequency on a daily or hourly basis for each week.

(Note that the time profile of virus and hack threats is automatically recorded by the network traffic sampler.)

3.4 Output

The output from the Activity Prediction is the predicted number of viruses and hacks for the next period. These numbers are shown in the bottom row of the table on the summary page. The model also stores the time, severity and target profiles for use in the Value at Risk calculation.

4 Value at Risk

4.1 Purpose

The Value at Risk (**VAR**) model combines the output from the Activity Prediction with knowledge of the IT **infrastructure**, its **processes**, **systems** and **dependencies**, to calculate the VAR to the enterprise. Like the activity prediction, it is also run in the background whenever necessary to keep the output current.

4.2 Define Infrastructure

Your main task for the VAR model is to define the corporate IT infrastructure so that the model can calculate the financial effect of successful **attacks**. This is done on the Define Infrastructure page.

The infrastructure consists of an interconnected tree of Processes, Systems and Categories. It is shown on the page as a diagram. You add items to the diagram by clicking a button on the toolbar to choose what to add (e.g. Add Process) then on the diagram at the place you want to add it. Notice that the status bar right at the bottom of the page contains a brief description of what you can do with the mouse in its current position (e.g. "Click to add new Process to diagram. Shift+Click to add more than one."). You can select and move objects on the diagram by clicking or dragging them with the mouse. The selected objects can be deleted using the Delete key or the toolbar button.

If the diagram gets too big for the screen, scrollbars appear on the sides. You can also zoom out (using the slider on the toolbar or Ctrl + mouse wheel) to get a wider view.

Categories sit at the root of the infrastructure tree. They represent things that may be the targets of an attack, such as particular pieces of software or a geographical location. A category has a vulnerability: this is the expected downtime caused by an attack of each severity level. Set this by selecting the category and entering the downtimes in the adjacent table.

A system is a particular piece of hardware, typically a server or cluster of servers. The most important information for n-ORM about systems is which categories they depend on, i.e. what possible attack targets they have. You define a dependency by holding down Shift and dragging an arrow from the system to the category it depends on. (This is also how you define dependencies between categories.)

Processes are continuous or regular activities undertaken by the business that have value to the business, for example, an e-commerce website. Processes depend on systems (the website would depend on the webserver, product database and credit card transaction processor, for example) for their operation. An attack that disrupts any one of its dependent systems will affect a process. Each process should depend on one or more systems; a system may have many processes depending on it.

Calculating the VAR requires processes to have a value assigned, defined as the hourly cost to the business of the process being unavailable. You enter this by selecting the process and typing the value in the adjacent table. The value of some processes may vary throughout the week. A business-to-business website serving one country may be of considerable value during the working

day, lower value at night and minimal value at weekends. This is accommodated by using a value profile with different values specified on a daily or hourly basis in the table.

The use of **Pages** to partition the infrastructure is described in section 5.1 Delegated Infrastructure below.

4.3 Variance from Baseline

n-ORM can monitor changes to the total VAR and show a warning if it deviates from an accepted baseline value. To use this facility, the baseline VAR and warning threshold must be defined. When the baseline scenario is configured and its VAR is shown, choose the acceptable variance from the drop-down list adjacent to the total VAR display then press the Accept as Baseline button. Subsequently, if changes to the scenario or threat environment increase the calculated VAR over the baseline figure, a warning is displayed on an amber background. If the calculated value exceeds the baseline by more than the acceptable variance, a stronger warning is shown on a red background.

The baseline VAR may be reset by pressing the Reset Baseline button; a new baseline and acceptable variance can then be defined.

4.4 Reports

The total VAR is shown towards the right of the summary page. To get more detail on the make-up of this figure, click the Reports button to bring up the VAR Reports page. This offers two alternative views on the data: by business process and a historical trend.

The VAR by Business Process tab allows you to see how the current VAR is divided among the processes or pages that constitute the infrastructure. The figures are shown in a table and bar chart. You can also filter the processes shown according to which page they occupy by clicking on the Filter button and highlighting the pages in the list that drops down (use Shift+Click to select a range of pages or Ctrl+Click to select individual pages).

The VAR Historical Trend tab shows you how the predicted VAR has changed over time as the threat environment and infrastructure evolve. You can see a summary of the data that led to a prediction in a panel underneath the VAR table. Click on a line in the table to update the panel.

5 Working across Multiple Sites

5.1 Delegated Infrastructure

As the **infrastructure** modelled in n-ORM becomes larger and more distributed, it becomes increasingly difficult for a single risk manager to accurately maintain. You can manage the complexity by drawing the infrastructure diagram on several **pages**. The pages have no significance to the n-ORM calculations, but act simply as a means of partitioning. You might find it convenient to have one page for each department or division, or perhaps one per data centre. Each **Process** should only appear on one page; **systems** and **categories** may be added to as many pages as required. An **attack** on a particular category will affect all categories with that name across all pages.

You can add or delete pages using a toolbar button or right-clicking on the page tab (only empty pages can be deleted). Right-clicking the tab also allows the page to be renamed or moved.

The next stage you can adopt is to delegate the maintenance of particular pages to someone more appropriate (e.g. the particular data centre manager). You export the page to a file (with the “.ipf” extension) and send the file to them. They have two ways to edit the file:

- a. **Using the full version of n-ORM.** (This option requires a licensing dongle.) They import the page file into their version of n-ORM, make any required changes and export it again.
- b. **Using the infrastructure editor.** (No license dongle required.) The page file can be opened using the infrastructure editor, edited there and saved again.

Either way, after making the changes, they send the file back to you and you import the page again. It will replace the existing page and update your infrastructure definition. You can use as many pages delegated to as many people as is necessary to manage your infrastructure.

5.2 Aggregated VAR

The above approach to managing diverse infrastructure still results in a single infrastructure being used in the calculations. All attacks will apply equally to the categories, whichever page they are on. Likewise, the same threat profile is assumed for all targets which may be a poor assumption for a global enterprise where different portions of the infrastructure are protected by different firewalls and subject to varying threat environments.

To model this case, it is best to manage each **location** that has a different threat environment using a separate installation of n-ORM. This will then sample the local threats and build an appropriate attack prediction for that location. Combined with the local infrastructure (which can be further delegated if appropriate), a VAR for that location can be generated. This local VAR is exported to a file (use the Export button on the summary page) with a “.nlv” extension and sent to a central place for combining with the VAR from other locations.

At the central office, you find the aggregate (global) VAR on the Aggregate VAR page. Use the button on the Imported VAR Locations tab to import all of the local VAR files required. The list shows you the VAR for each location and when it was generated.

To drill down into the data, switch to the Aggregate VAR tab. There, you can choose to show a table and chart of the VAR by location, page within each location or process.

The aggregated data can be exported to a file in XML format for input into other tools. Clicking the “Export to XML” button will launch a save dialog in which the name and location of the file to export to can be specified or an existing file selected. If an existing file is selected, an overwrite-file confirmation prompt will be displayed. Selecting ‘yes’ will destroy any data currently in the selected file.

6 Other Tasks

6.1 Audit History

All changes that you make to the **scenario** data are logged with your user name and the time the change was made. You can view the changes that have been made on the Scenario Change History page, accessible from the summary page. A tree on the page shows the user and time of each set of changes. To see the changes made, expand the nodes of the tree to the required level of detail.

6.2 Non-interactive Mode

You may wish to have n-ORM perform its calculations automatically on a recurring basis or as part of a chain of tools, without requiring user intervention or displaying its graphical interface. This may be achieved by adding the `-NonInteractive` switch to the command line used to start the program (e.g. `C:\Program Files\n-ORM\n-ORM.exe -NonInteractive`). To prepare for non-interactive operation, you should run n-ORM in the normal interactive mode and specify the scenario that will be used and the output location on the configuration page. When n-ORM is run non-interactively, it reads the scenario file, performs the calculations and places the output in the directory you specified earlier.

Running n-ORM on a scheduled basis depends on your operating system – you create a Scheduled Task under Windows, or use a cron job under Linux. Consult your system administrator to set this up.

7 Glossary

Aggregated VAR	The combined VAR from several locations .
Attack	Overarching term for Virus , Hack and Physical Threat . If an attack is successful, it causes downtime to all Systems in a System Category according to its severity and their vulnerability.
Business Process	See Process .
Business System	See System .
Category	A common characteristic of a set of Systems that may be subject to attack (virus , hack or physical). The commonality may be software running on the Systems, the geographical location of the Systems or another factor. For example, Windows Server 2003 R2 or London data centre.
Dependency	Within the infrastructure , Processes depend on Systems (implying that the system must be working for the process to operate). In turn, systems depend on System Categories (see Category for interpretation). Categories may also depend on each other in certain cases: for example, a System might depend on the Windows Server 2003 category, which in turn depends on the Windows category. In that case, any successful attack on Windows would also damage systems in the Windows Server 2003 category.
Hack	Generic term for an electronic attack to the network, specifically targeted at the organisation, for example port scanning, denial-of-service, etc. See also virus , physical threat .
Infrastructure	The Processes , Systems and Categories that represent the corporate IT network and its applications, together with their inter dependencies .
Location	Part of the enterprise whose infrastructure is assumed to be subject to a common threat environment. The VAR at each location is calculated separately and may be combined into an aggregated VAR .
Page	A subset of the infrastructure at a location . Pages can be exported and imported to allow their maintenance to be delegated.
Physical Threat	A non-electronic threat to the network, such as fire, flood, theft, terrorism, etc. This type of attack must be entered manually as they cannot be estimated from network traffic. See also virus , hack .
Portfolio	A collection of related scenarios consisting of a baseline and (optionally) one or more variations.
Process	An activity performed by the business using one or more Systems that has a defined value to the business. For example, sending new product emails which depends on the customer database and the email server.
Scenario	A combination of Infrastructure and Physical Threats . These are used together with the currently predicted virus and hack threats to calculate the corporate Value at Risk .

System	A piece of hardware which supports one or more Processes to run the business. It belongs to one or more Categories which may be subject to attack . For example, the customer database might belong to the Oracle, Windows Server 2003 R2 and London data centre categories.
System Category	See Category .
VAR	Value at risk. The best estimate of the expected cost to the enterprise of attacks to its IT infrastructure .
Virus	Generic term for an electronic attack to the network, not specifically targeted at one organisation. Covers viruses, Trojans, worms, etc. See also hack , physical threat .