



**Quantar**  
**SOLUTIONS LTD**  
Network Risk Valuation

# *n-ORM*<sup>TM</sup>

*Network Operational Risk Manager*

measuring the unknown

# Network Operational Risk Manager

## Quickly deployed, effective network operational risk valuation and management software

n-ORM is the industry's risk management integrated network operational risk valuation solution for the identification, quantification, assessment and valuation of the threats to enterprises arising from internet connectivity. n-ORM enables rapid deployment of a fully-functional methodology to evaluate the risks posed to company-specific systems & business operations & to assess the cost-benefit of implementing mitigation options. Flexibility & ease of use reduces cost of ownership & training requirements.

### Network Operational Risk Manager

Network operational risks cannot be managed successfully using simplistic models and spreadsheets due to the specificity of this type of risk. In effective management of this type of risk, organisations need to understand both the interconnectedness of business operations and the continual evolution of the risks created by the internet.

Relying upon historic data to manage network operational risks is a major failing in many organisations, who fail to take into account the rate of evolution of threats, together with an increasing trend towards targeted attacks upon organisations.

Deploying n-ORM within an organisation is quick, and with a low training requirement, together with widespread

usage of the system output, organisations can leverage n-ORM to create a more risk-aware culture from within.

One of the greatest business risks facing companies today is that of non-compliance with an ever-increasing number of regulatory requirements. While many currently strive to meet current standards, they are ill-equipped to face the wave of new regulations implemented around the world, reducing competitive ability.

Only a simple to use, effective and accurate reporting system for network risks can enable internal audit and compliance teams to facilitate companies adherence both to today's and future reporting requirements. Mistakes will be costly, ranging from financial penalties to reputational damage.

.....with n-ORM regulatory risks can be managed effectively today and in the future....



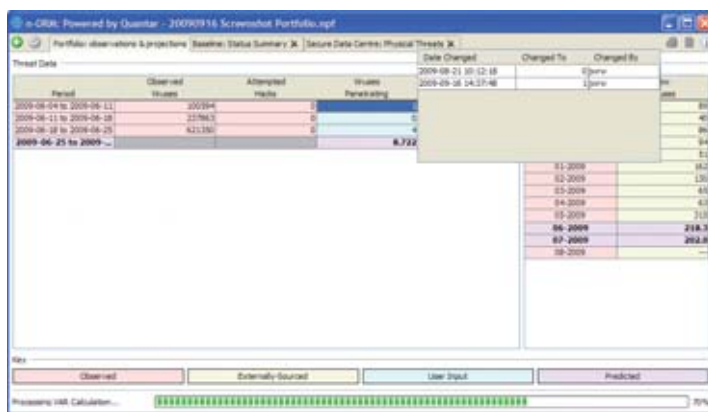
# Network Operational Risk Manager

## Solution Overview

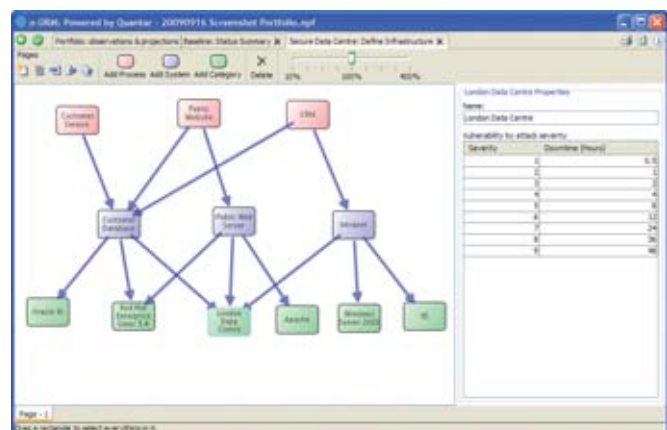
Quantar's network operational risk manager (n-ORM) is a two-part risk management system that collects, aggregates, processes and reports on the value at risk arising from the interconnectedness of an organisation's private network with the internet. It utilises standards-based software architecture.

### Modules:

- Capital Modelling:** n-ORM's capital modelling provides a bottom-up method for aggregating loss calculations and facilitates assessment of the cost-benefit of undertaking risk management of network risks, for effective information risk management.
- System Configurator:** Offers user-defined parameter settings for the location of scenarios, threat data location, currencies, time zone, language options, and the period for which the value at risk output should be displayed.
- Process Manager:** GUI based module facilitating business process mapping against an organisations systems and categories. User-defined inputs for severity versus downtime per category, together with outsourcing weightings and process profile, enables a high degree of granularity as well as achieving high accuracy in business process mapping. As a stand-alone component, Process Manager may be dispersed through an organisation to various business units and departments and aggregated within a centrally run n-ORM solution or on an individual basis for per unit value at risk calculations.
- Physical Attack Configurator:** User-defined types of attack that impact upon the degree of resilience that impact upon an organisation within the context of network risks, such as flooding and fire.
- Reports Module:** Visual overview of the organisation's value at risk status, with filtering and historical trend analysis, per process or page, with print functionality and scenario import options.
- Scenario module:** Change history for all parameters within the solution, with print functionality and import capability. Provides complete transparency for audit and compliance teams and regulators.
- Multi-language Capability:** The system is delivered in English and Arabic, with a further option for it to be supplied in others at an additional development cost.



Portfolio: projections and observations



Process Manager: systems; processes and categories

# Network Operational Risk Manager

## What does Quantar's n-ORM do?

As a system developed to quantify the risks faced by organisations from internet threats, n-ORM helps companies meet and adapt to numerous regulatory compliance mandates, as well as serving internal risk management requirements. The system's self-documenting threat data and user defined parameter changes automates the entire audit requirements for transparency, whilst affording risk managers a detailed overview of the organisation's network operational risk management effectiveness.

## Why should n-ORM be important to businesses?

n-ORM assists organisations in the measurement and valuation of network threats

arising from the internet in a structured and empirical way, and not simply for regulatory compliance purposes, but to develop and maintain business continuity and full enterprise resilience.

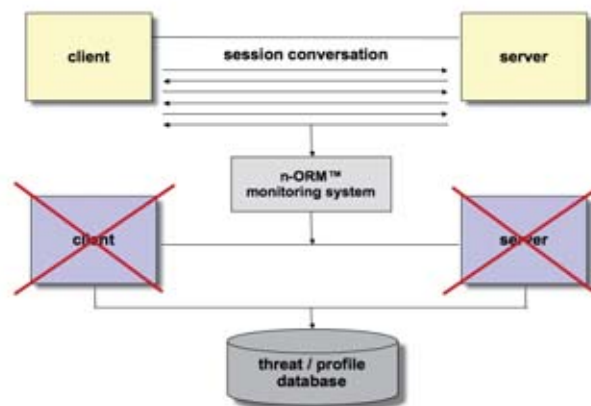
## Who should use n-ORM?

n-ORM has been developed for all organisations seeking to achieve business sustainability through effective management of internet threats, whether through IT security enhancements, insurance risk mitigation or

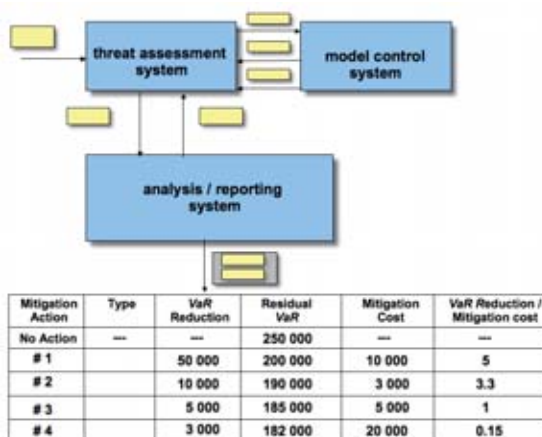
any other risk management techniques.

Governmental and non-Governmental organisations may use n-ORM as part of their critical infrastructure protection programmes

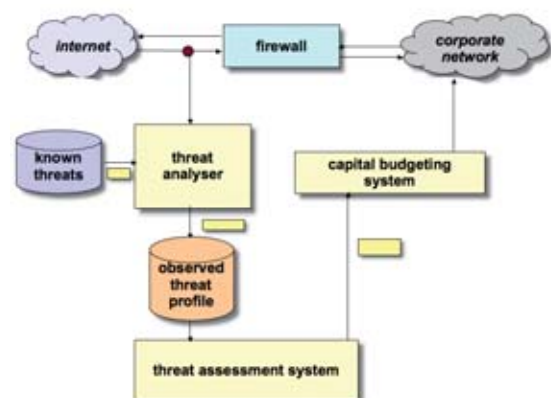
All stakeholders within organisations; risk managers, business managers, network security professionals, audit managers, etc. can utilise the output from n-ORM for their individual requirements.



n-ORM copies patterns in traffic, NOT the information in the traffic. A patented methodology.



n-ORM system front-end captures back-end data and combines with user defined parameters and external data to deliver clear value at risk data.



n-ORM installation point is outside of the corporate network, assessing inbound traffic patterns for threats

# Network Operational Risk Manager

## Key Benefits

With n-ORM, organisations can:

Implement a self-documenting network risk valuation infrastructure that integrates network threat data and company specific data into a single repository for risk management and compliance reporting.

Adopt a consistent network operational value at risk methodology throughout an organisation, regardless of size or location

Create a group-wide overview of network operational risks facing the organisation, regardless of language or currency.

Provide the level of transparency and traceability that is increasingly required across a number of sectors by regulatory authorities.

Enhance the cost-effectiveness of risk management actions through the n-ORM capital budgeting function by tracking progress towards the desired value at risk reduction whilst determining the cost-benefit of each risk mitigant.

Network Operational Risk Manager (n-ORM) from Quantar is a scalable, cost-effective solution designed to assist organisations in managing threats posed by their private networks being linked to the internet.

n-ORM identifies, measures and values network operational threats as well as providing effectiveness measurements for mitigation actions an organisation may seek to take in successfully

```
<?xml version="1.0" encoding="UTF-8"?>
<Crimson Version="1">
  <ObservedThreats ObservationStart="2009-03-16T00:00:00" ObservationEnd="2009-03-23T00:00:00">
    <Threat ID="1408" Category="Indiscriminate" Target="Unknown" SeverityScore="7">
      <Observation Day="Monday" From="00:00:00" To="00:59:59" Count="100"/>
      <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="115"/>
      <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="90"/>
      <Observation Day="Monday" From="03:00:00" To="03:59:59" Count="110"/>
      <Observation Day="Monday" From="04:00:00" To="04:59:59" Count="110"/>
      <Observation Day="Monday" From="05:00:00" To="05:59:59" Count="70"/>
      <Observation Day="Monday" From="06:00:00" To="06:59:59" Count="110"/>
      <Observation Day="Monday" From="07:00:00" To="07:59:59" Count="170"/>
      <Observation Day="Monday" From="08:00:00" To="08:59:59" Count="80"/>
      <Observation Day="Monday" From="09:00:00" To="09:59:59" Count="135"/>
      <Observation Day="Monday" From="10:00:00" To="10:59:59" Count="155"/>
      <Observation Day="Monday" From="11:00:00" To="11:59:59" Count="150"/>
      <Observation Day="Monday" From="12:00:00" To="12:59:59" Count="130"/>
      <Observation Day="Monday" From="13:00:00" To="13:59:59" Count="120"/>
      <Observation Day="Monday" From="14:00:00" To="14:59:59" Count="150"/>
      <Observation Day="Monday" From="15:00:00" To="15:59:59" Count="85"/>
      <Observation Day="Monday" From="16:00:00" To="16:59:59" Count="210"/>
      <Observation Day="Monday" From="17:00:00" To="17:59:59" Count="140"/>
      <Observation Day="Monday" From="18:00:00" To="18:59:59" Count="180"/>
      <Observation Day="Monday" From="19:00:00" To="19:59:59" Count="145"/>
      <Observation Day="Monday" From="20:00:00" To="20:59:59" Count="110"/>
      <Observation Day="Monday" From="21:00:00" To="21:59:59" Count="160"/>
      <Observation Day="Monday" From="22:00:00" To="22:59:59" Count="90"/>
      <Observation Day="Monday" From="23:00:00" To="23:59:59" Count="155"/>
      <Observation Day="Tuesday" From="00:00:00" To="00:59:59" Count="110"/>
      <Observation Day="Tuesday" From="01:00:00" To="01:59:59" Count="85"/>
      <Observation Day="Tuesday" From="02:00:00" To="02:59:59" Count="145"/>
    </Threat ID="1408">
  </ObservedThreats>
</Crimson Version="1">
```

Sample of actual threat data generated by n-ORM

meeting its regulatory, governance and compliance goals.

Designed to capture organisation-specific threat data and to combine this with externally sourced data and user-defined inputs, n-ORM helps business units and risk management teams optimise their information security policies and procedures.

With the ability to export to files in, n-ORM may be used in conjunction with other risk management tools and systems, with no further development

required, creating a cost-effective means of assessing total enterprise resilience status.

Data theft or loss has become, for the first time in history, one of the leading global threats identified by the World Economic Forum (Davos 2009).

With organisations investing heavily in information technology and resources, in support of existing business operations, or to enhance profitability and competitive advantage, interdependencies are increasing in volume and complexity.

### Can your organisation:

1. determine the risk exposure of critical assets and business processes?
2. accurately prioritise which risk management options will reduce the exposure to the required level?
3. identify the most cost-effective risk management options to manage your network threats?

# Network Operational Risk Manager

## Network Operational Risk Manager Advantage

With the capability to export the output from n-ORM in xml format, the system can be integrated into other solutions or even directly into a spreadsheet. This approach to development ensures the flexibility needed by many organisations in their ongoing risk management programs and to meet changing regulatory requirements.

The current climate of regulation and control, together with increasing legal requirements, has pushed risk management and business continuity out from a niche within organisations to business units and senior management. Simultaneously, the forces of market pressure to increase profitability through enhanced efficiencies without compromising performance through errors and omissions brings greater complexity to management and control.

Taking control of your network operational risks through utilising n-ORM, your organisation may, through the mapping of business processes and

interconnectedness of processes, systems and categories, find an unexpected bonus – increased process efficiencies. Enhancing an organisation's risk management practices can often improve overall business performance.

With ever-increasing compliance requirements, the ability to record and report how and why a value at risk arising from network operational dependencies is arrived at makes an audit team's ongoing task simple and transparent. n-ORM's reporting functionality is sufficiently detailed to make regulatory compliance less of a burden and helps

organisations develop a historic basis for its' compliance reporting.

With a simple, dependable and accurate means of quantifying your organisation's network operational risks, n-ORM reduces the total cost of ownership, whilst enhancing overall risk management effectiveness.

User defined inputs, combined with observed and externally sourced data address client-specific network operational risk management needs, without the need for external parties or expensive additional system development and deployment requirements.

### CSI/FBI Computer Crime and Internet Security Report 2008 (522 Respondents):

Average financial loss per computer fraud: \$500 000

Dealing with 'BOT PC's within an organisation: \$350 000

Overall average loss per loss: \$300 000

27% experienced targeted attacks against the organisation

68% of organisations have information security policies;

18% were developing them; only 1% had none.

29% Denial of service attacks

29% Unauthorised Access

50% Virus attacks

12% Financial Fraud

13% System penetration

9% Theft/loss of proprietary information

20% BOTS

17% Theft/loss of customer data

8% DNS attacks

9% Password sniffing

# Network Operational Risk Manager

## Key Points Summary

- n-ORM quantifies network risks, utilises both automated data and user-defined inputs to arrive at the risk exposure of your organisation taking into account systems, processes and dependencies in a simple and effective manner.

- n-ORM automates the risk quantification process, providing a unified value at risk calculation for network operational risks facing the organisation, enabling proactive and pre-emptive risk management.

- n-ORM's Infrastructure Manager, built on the n-ORM platform, enables risk managers to map the organisation's business processes, systems and dependencies in unlimited numbers of locations and aggregate them into a

single value at risk for the organisation, or to review multiple locations on an individual or batch basis.

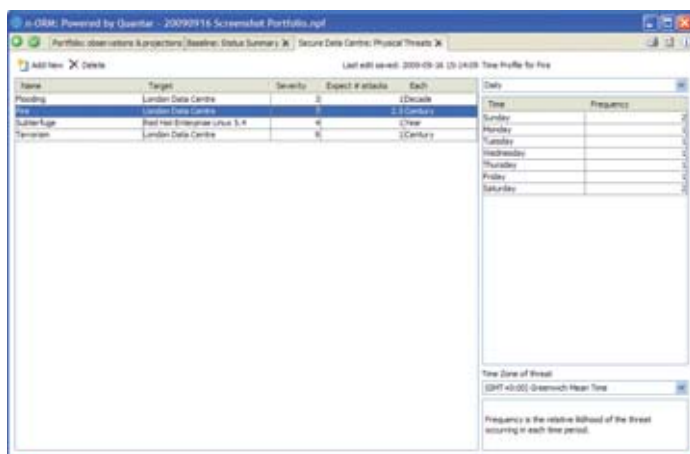
- n-ORM is designed to help companies to collect, analyse, assess and report on network operational risks for the benefit of long-term enterprise resilience and business continuity. Institutions can rapidly deploy n-ORM without the need for expensive customisation, and with minimal organisational resources.

- n-ORM is a unique organisation-centric solution to network operational risk, overcoming the traditional problems associated with a silo or location-based approach to the identification and quantification of network threats. Individual or multiple location ability means that risk management teams can

provide detailed information per office/geography /SBU to internal management and to regulators.

- n-ORM enables users to be able to view and report on historical analysis and trends over time, thereby providing enhanced capability to optimise risk management and business continuity solutions as well as providing a transparent audit trail.

- n-ORM has been designed to give end users the ability to effectively manage, measure and control those risks brought to organisations by the internet and threaten enterprise resilience and business continuity in a simple to use and understand way. With n-ORM, complying with operational risk and corporate governance regulations has taken a step forward in simplifying a complex task.



n-ORM Physical Threats Configuration Utility



Portfolio analysis with mitigation effects on value at risk (VaR)

# Network Operational Risk Manager

## Service Support

Quantar Solutions offers three levels of service support for its Network Operational Risk Manager application. Customers may specify at the time of purchase the desired level of service most appropriate for their organisation. Additionally we are able to offer individual solutions on a case-by-case basis upon request.

First level Service Support is provided by the n-ORM Support Portal, which enables customers to file incident and/or service requests to our technical support teams. In all instances, the Support Portal is the first point of contact, and provides a full transparent view on the processing status of your request at any time. You may also reduce the time to recover any n-ORM incident by uploading helpful information, such as the

system error log files. All reported service requests can be tracked, validated with the support team, prioritised and even closed via the n-ORM Support Portal.

With the Gold service level, we will call your organisation back on demand. All that is necessary for incidents and/or service requests is for the initial recording of it/them to be made via the n-ORM Support Portal.

## About Quantar Solutions Ltd

Quantar Ltd was established in 2000 following from initial collaborative developments with a number of third party organisations in the computer security and reinsurance fields. Expertise in the areas of risk management and enterprise resilience, including consequential damage arising from security breaches has been the mainstay of the organisation since its establishment. We also have extensive experience in the fields of corporate communications, research and technology implementation.

Quantar Solutions Ltd is a corporate partner of the Business Continuity Institute.

For Further Information Contact:

Quantar Solutions Ltd  
St. John's Innovation Centre  
Cowley Road  
Cambridge  
CB4 0WS  
UK

Tel: +44 1223 422238  
Fax: +44 1223 420844  
e-mail: [info@quantarsolutions.co.uk](mailto:info@quantarsolutions.co.uk)  
<http://www.quantarsolutions.com>



© Quantar Solutions Ltd 2009