



n-ORM™ Presentation

Dr. Phillippe Evrard

A Brief Background to Swiss Re & Us

First approached Swiss Re in 2001 to seek out underwriting expertise in the area of network security and emerging digital risks

Post-meeting development of methodology and refining technical systems and software development

Ongoing emerging risks and network security developments drive updated methodology and front-end developments utilising best in class third parties – NSC / LUEL / Venner Shipley / LCP

Development History

1998 – 2000 Initial methodology of traffic capture in a covert manner first developed

2000 – 2004 Meetings with re-insurers; IT security suppliers; risk management systems developers + refinement of capture + international patent filing (PCT)

2005 – 2008 External development of back-end and front end by leading edge consultants to create commercial product

2008 – 2009 Field trials leading European Group of banks/insurers + review of methodology by award winning actuarial consultancy + enhanced integration between back-end and front end.

What is it for?

Objective:

to use external independent data allied to company-specific data and user inputs to determine the value at risk arising from business operations built upon IT/network dependence.

Risk Management:

to provide the means by which senior management may manage; eliminate; mitigate risks arising from IT/network infrastructure or how business operations integrate/interact with it.

Audit/Compliance:

increasing global regulatory requirements and a need for an accepted method of valuing network/IT risks linked to business operations

What are we looking for?

1. A risk carrier who is able to underwrite the following risks:
 - a. Business interruption based upon the model
 - b. Reputational damage risks arising from business interruption and/or or defaced corporate website/s
 - c. Limited product liability cover (excess covered by 'shrink-wrap' disclaimer)
2. Additionally, possible co-development of the underwriting methodologies over time as technology and business operations shift
3. Insurance product development partner/s for specific network digital risks
4. Potential partnering for product distribution

Swiss Re Coverage in Alignment

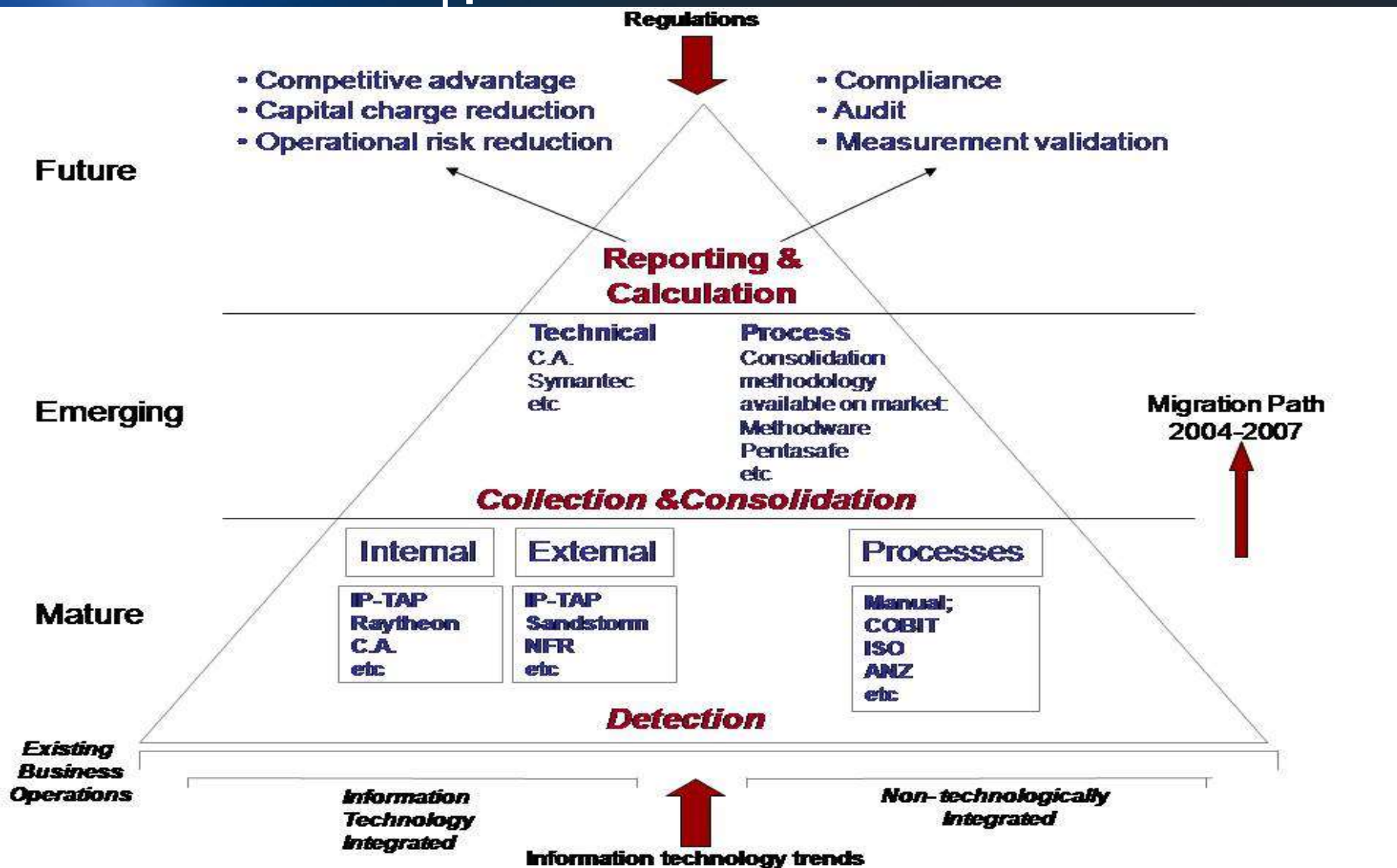
Swiss Re are already active within the same segment/cover/activities:

- Specialist crime policies and extensions, covering, for example, **electronic/ computer crime**, plastic cards, extortion, Assurance/Insurance company forgery risks, ATMs and mortgage fraud
- Cover to mitigate an institution's financial exposure to **Operational Risks**, which is of particular importance in the light of the **Basel Capital Allocation** requirements

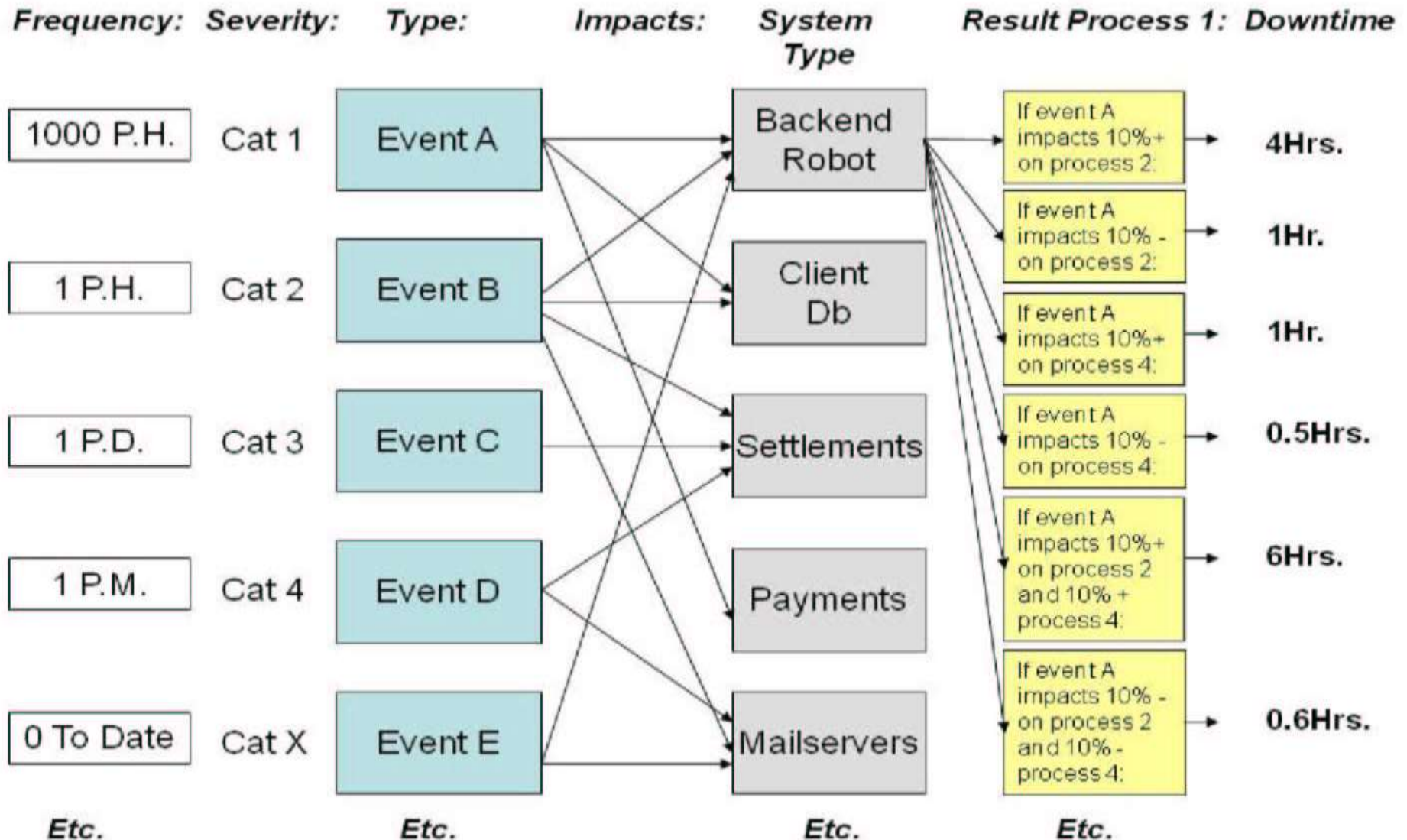
The New Environment

- Banks – *mandated* under Basel II to quantify and value operational risks
- Insurance *mandated* under Solvency II to quantify and value operational risks
- Companies listed in the U.S. *mandated* under SOX to quantify and value operational risks
- All major companies, across various sectors active in risk management programmes
- All companies increasingly seeking to create an internal risk-aware organisational culture.

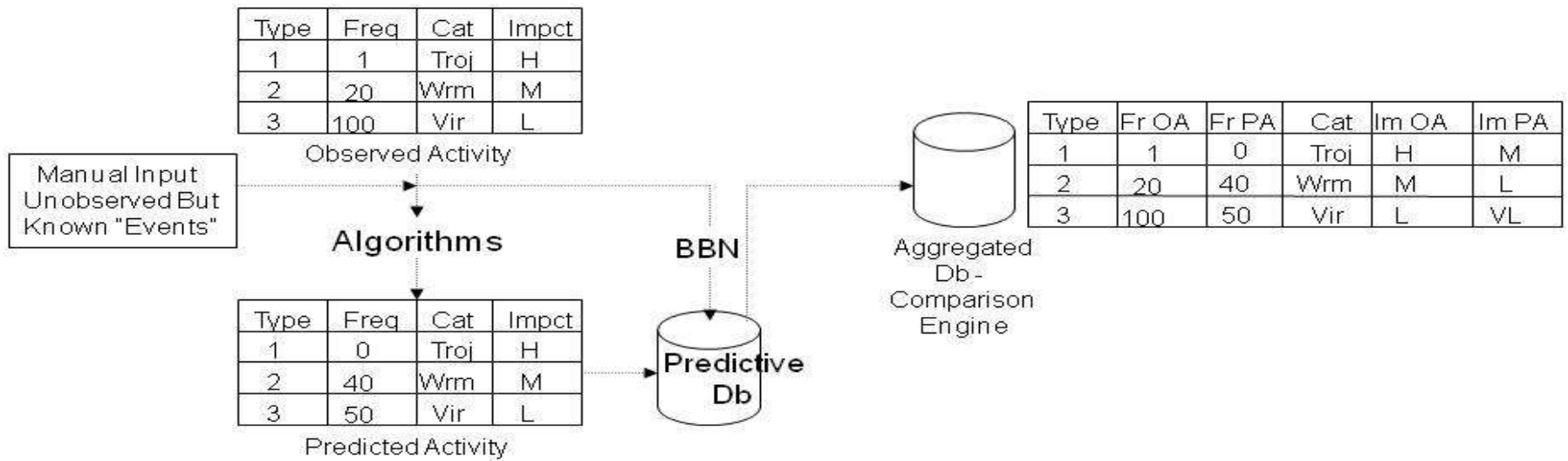
The New Environment



Overview (1)



Overview (2)



Manually Entered Variables

Event Type	Process No.	Criticality	Process Interdependence	% Dep.	% Mitigation Reduction	Probability of Mitigation	Totals
1	1a	1	1b	50	0	0	
			4c	10	50	2	
			7a	2	5	10	
2	1b	3					
3	2a	1					

The Algorithmic Models

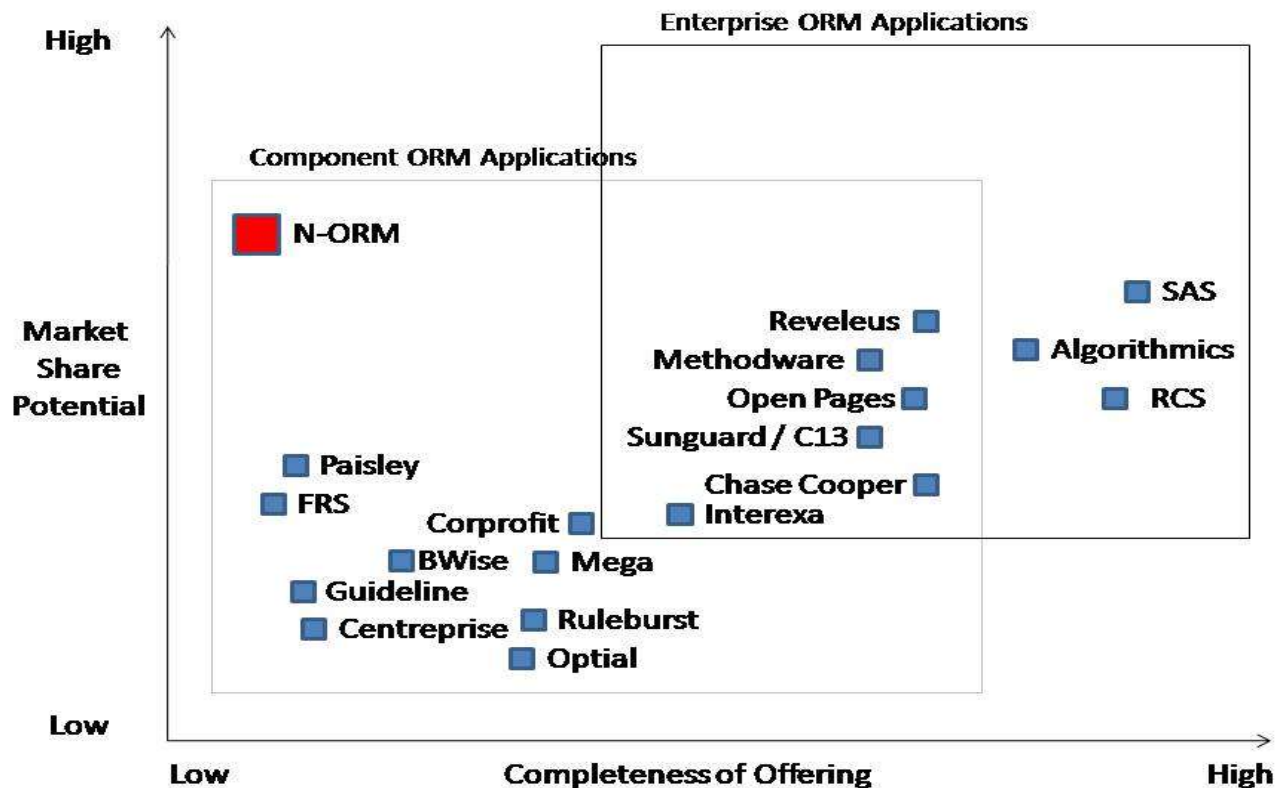
- Investigation undertaken (by 2 separate external companies) into the most appropriate based upon test data
- Options were: Weighted Linear Extrapolation; Bayesian Networks; Markov Model; Autoregression.
- Selection based upon a simple approach for customers and Supervisors to understand as well as best fit to trial data.
- Autoregression may be implemented with greater volumes of data to test
- Future development will offer optional modelling methods

Risk Management Systems Trends

3 types of players in the market:

- largescale organisations such as Oracle ; SAP ; IBM with add-ons for their ERM and other platforms
- middle market players, such as SAS & Algorithmics
- small players targeting niche markets, such as Popkin; Amelia; Paisley; Coreprofit, etc
- products aimed at either internal usage and controls and external usage for audit and compliance
- activity coverage ranges across the board- from treasury to credit, to political to COBIT

Overall Landscape for Risk Management Applications



Source: Charis Research Report #RR0701 – Operational Risk Management Systems 2007

What is n-ORM™?

- n-ORM comprises 2 (globally patented) elements;
 - a) a traffic collector (back-end)
 - b) a system that quantifies the value at risk arising from connecting a corporate network to the internet (front-end)
- It is a compliance tool for Basel II / SOX / Solvency II / Other regulations
- A risk assessment tool as part of an overall risk management methodology
- A means of creating a sectoral loss database
- The methodology to enable underwriting of these risks

What is nOpVaR™?

- The output from n-ORM labelled network operational value at risk (nOpVaR™).
- Derived from data + algorithmic models within the n-ORM / data capture systems
- Company-specific / unit-specific configured output derived from a combination of automated internal / external data and manually input data
- A monetary value to be used within the overall risk assessment program of an organization.

Current Product/Service Offering

- Complete system
- Volume pricing licensing for 'process manager' element
- Consultancy based upon initial installation, configuration and training
- Subsequent consultancy based upon third party validation of *VaR* attributed
- System has audit/control report functionality for regulatory compliance
- Historical data analysis for accurate assessment and valuation of risk

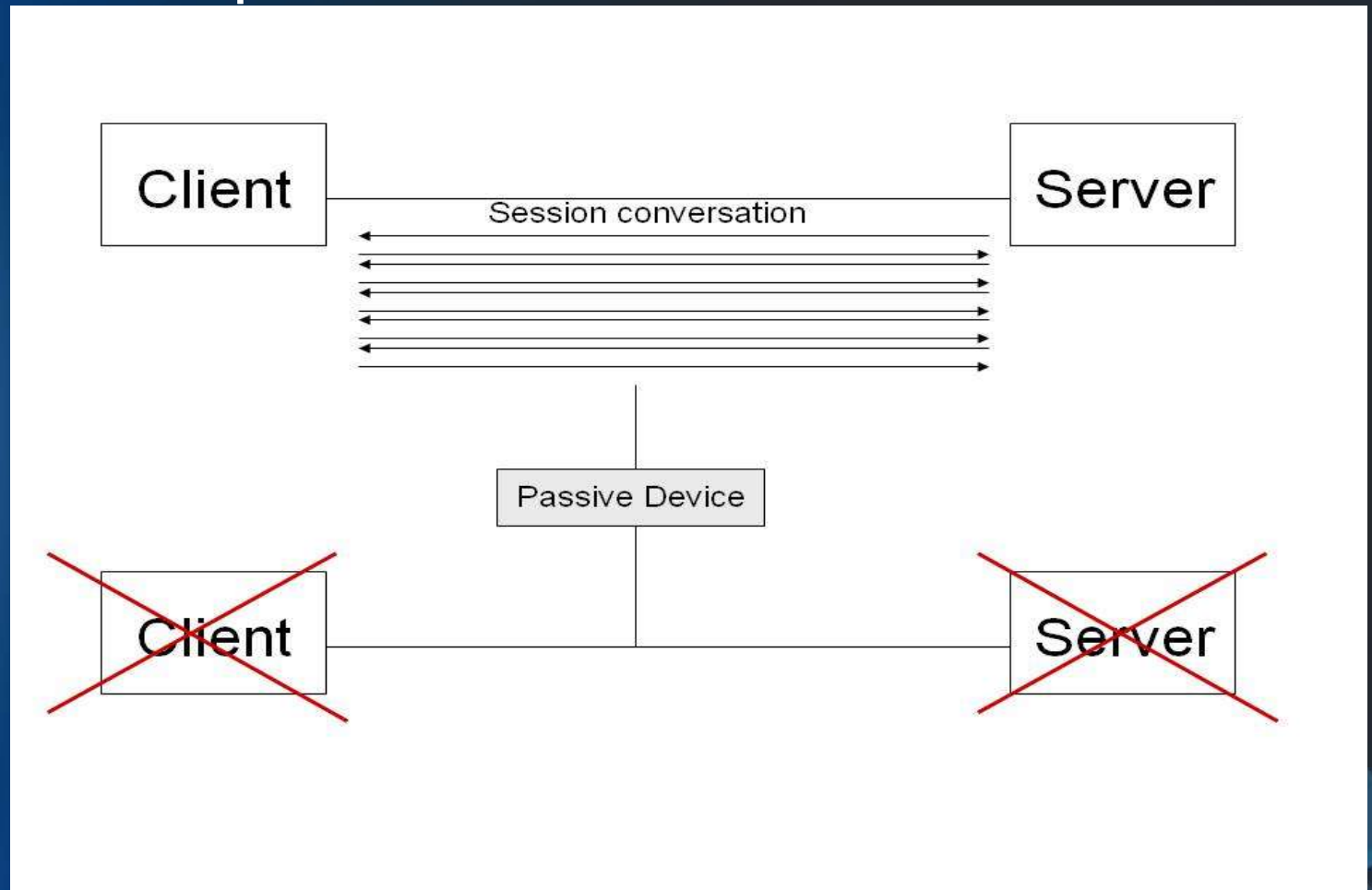
Current Modules / Options

- Full version including front & back-ends; dongle to unlock the limitations on the front end
- Trial version with limited parameters and time-scales
- Stand-alone process manager – multiple process manager modules may be imported to arrive at an aggregated total *VaR*
- Language support. Currently English; Spanish; Arabic

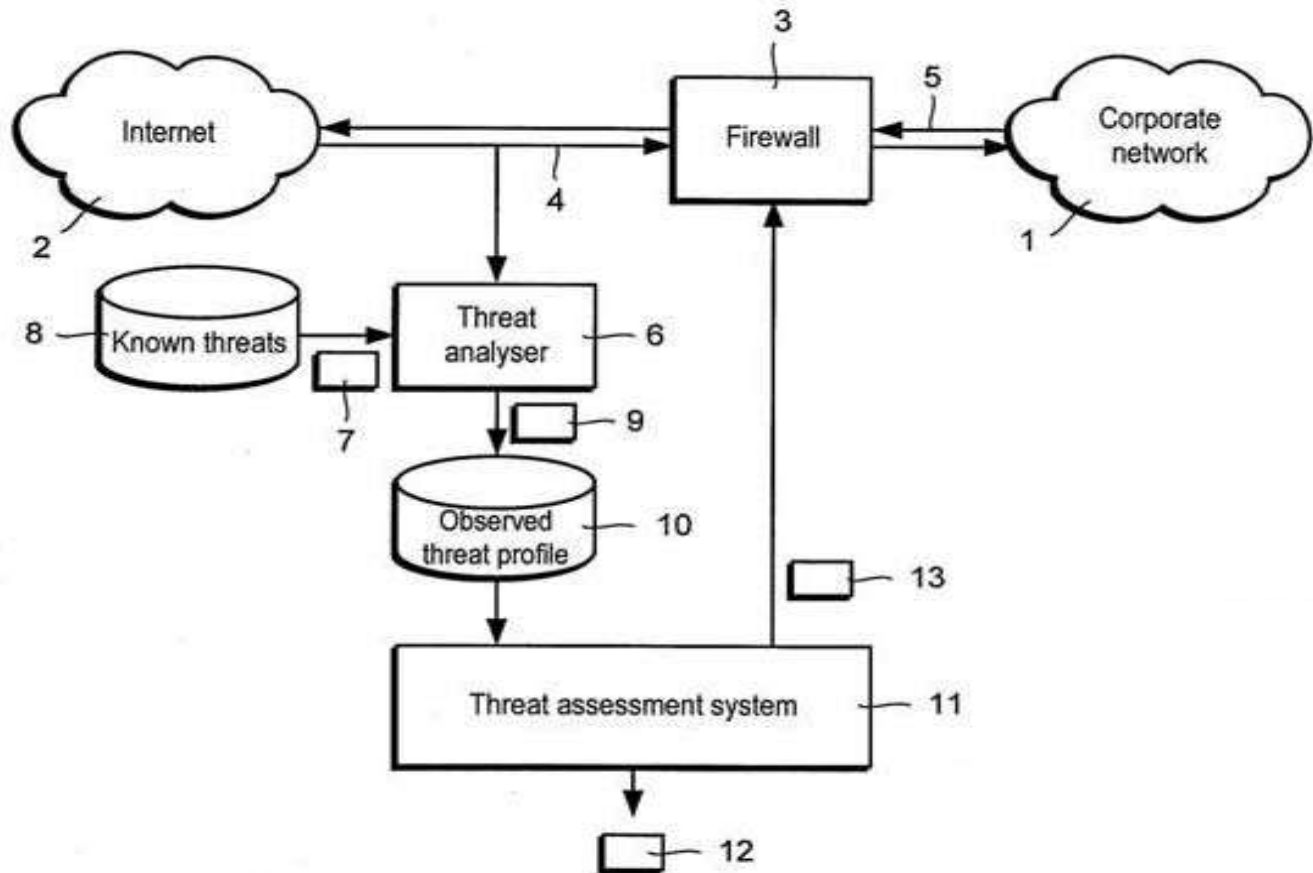
Future Product/Service Offering Additions

- Risk coverage (insurance / risk financing) based upon system *VaR* output
- Measurement against sectoral loss database (subscription model as per certain company's Db's)
- Multiple measurement models as optional risk management tools (option to use most appropriate for internal requirements versus reg. compliance)
- Varying types of coverage taking multiple inputs (system and organisation-specific)

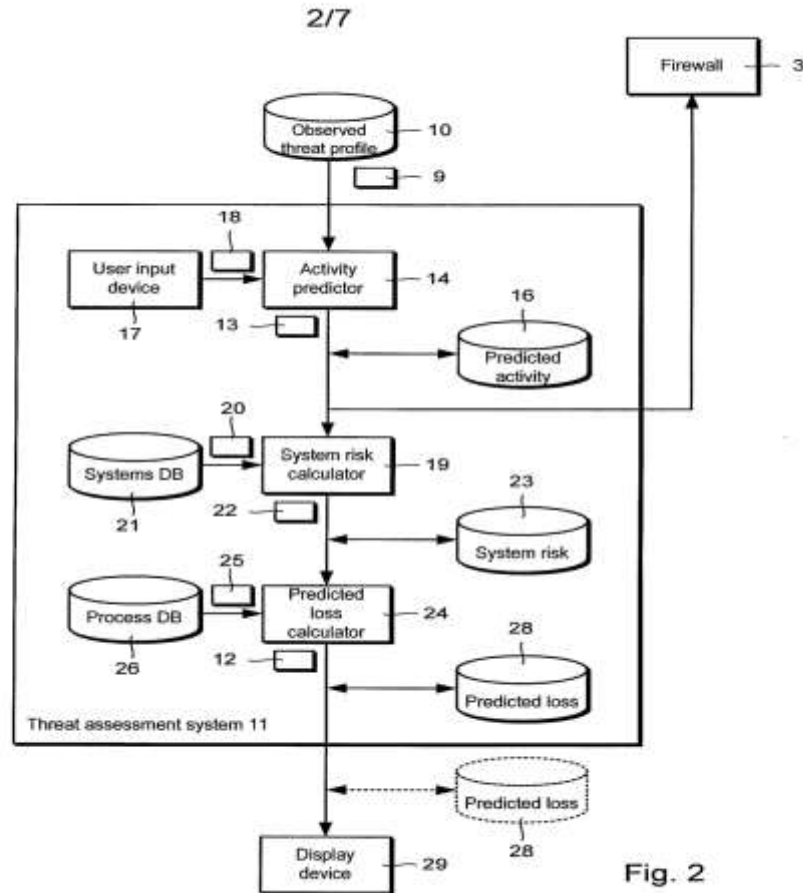
Basic Copy Model



Installation Positioning



System (2)



System (3)

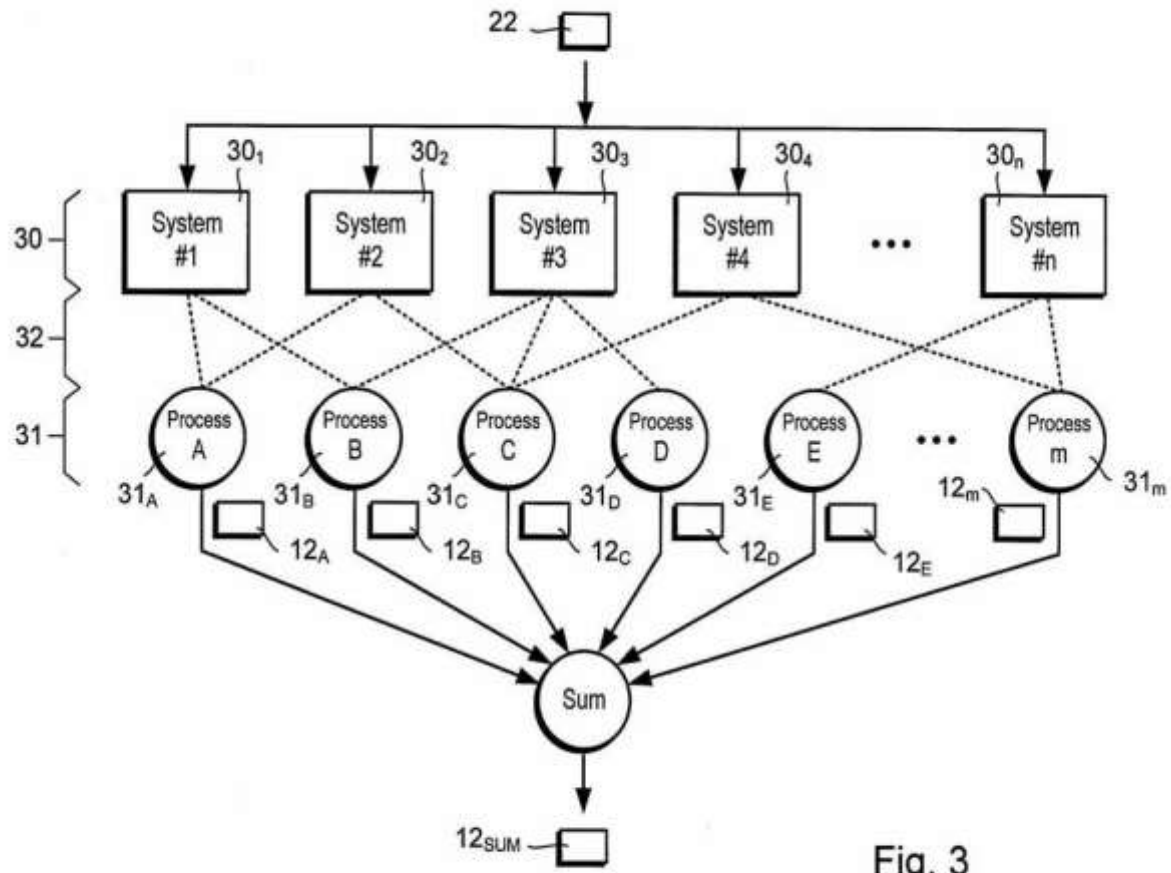


Fig. 3

XML Threat Data

- `<Crimson Version="1">–`
- `<ObservedThreats ObservationStart="2008-02-25T00:00:00" ObservationEnd="2008-03-03T00:00:00">`
- `<Threat ID="DOS MSDTC attempt" Category="Indiscriminate" Target="Unknown" SeverityScore="7">`
- `<Observation Day="Monday" From="00:00:00" To="00:59:59" Count="52"/>`
- `<Observation Day="Monday" From="01:00:00" To="01:59:59" Count="32"/>`
- `<Observation Day="Monday" From="02:00:00" To="02:59:59" Count="56"/>`
- `<Threat ID="WEB-MISC http directory traversal" Category="Indiscriminate" Target="Unknown" SeverityScore="7">`
- `<Observation Day="Monday" From="00:00:00" To="00:59:59" Count="247"/>`
- `<Observation Day="Monday" From="01:00:00" To="01:59:59" Count="152"/>`
- `<Observation Day="Monday" From="02:00:00" To="02:59:59" Count="266"/>`
- `<Observation Day="Monday" From="03:00:00" To="03:59:59" Count="437"/>`

What Does the Threat Data Mean?

- `<Crimson Version="1">-`
- `<ObservedThreats ObservationStart="2008-02-25T00:00:00" ObservationEnd="2008-03-03T00:00:00">`
- `<Threat ID="DOS MSDTC attempt" Category="Indiscriminate" Target="Unknown" SeverityScore="7">`
- `<Observation Day="Monday" From="00:00:00" To="00:59:59" Count="52"/>`
- `<Observation Day="Monday" From="01:00:00" To="01:59:59" Count="32"/>`
- `<Observation Day="Monday" From="02:00:00" To="02:59:59" Count="56"/>`
- `<Threat ID="WEB-MISC http directory traversal" Category="Indiscriminate" Target="Unknown" SeverityScore="7">`
- `<Observation Day="Monday" From="00:00:00" To="00:59:59" Count="247"/>`
- `<Observation Day="Monday" From="01:00:00" To="01:59:59" Count="152"/>`
- `<Observation Day="Monday" From="02:00:00" To="02:59:59" Count="266"/>`
- `<Observation Day="Monday" From="03:00:00" To="03:59:59" Count="437"/>`

Main Screen

- Gives a total aggregated risk and value at risk
- Simple to understand
- Audit and compliance focussed
- Reporting and record maintenance of changes create clarity to Supervisors
- Intuitive ease of use requires little training
- Multiple options in the calibration of basic inputs, such as currency, language

The Main Screen

n-ORM: Powered by IP-TAP - Scenario.nsf

Status Summary

Define: Physical Attacks | Infrastructure | Reports | Aggregate | Export | Change History: Scenario | Incidents

Threat Data

Period	Observed Viruses	Attempted Hacks	Viruses Penetrating		Successful Hacks	Physical Attacks	New Viruses	
							Month	New Viruses
2006-07-31 to 2006-08-07	4715	4258	0	0	0	09-1997	5	
2006-08-07 to 2006-08-14	4056	4807	0	0	0	10-1997	2	
2006-08-14 to 2006-08-21	4854	4388	0	0	0	11-1997	8	
2006-08-21 to 2006-08-28	4723	4492	0	0	0	12-1997	9	
2006-08-28 to 2006-09-04	4627	4415	0	0	0	01-1998	2	
2006-09-04 to 2006-09-11	4116	4825	0	0	0	02-1998	4	
2006-09-11 to 2006-09-18	5011	3970	0	0	0	03-1998	2	
2006-09-18 to 2006-09-25	4559	4494	0	0	0	04-1998	3	
2006-09-25 to 2006-10-02	4461	4489	0	0	0	05-1998	0	
2006-10-02 to 2006-10-09	4128	4693	0	0	0	06-1998	2	
2006-10-09 to 2006-10-16	4235	4666	0	0	0	07-1998	7	
2006-10-16 to 2006-10-23	5110	4176	0	0	0	08-1998	3	
2006-10-23 to 2006-10-30	4580	4409	0	0	0	09-1998	---	
2006-10-30 to 2006-11-06	4571	4417	0	0	0	10-1998	1	
2006-11-06 to 2006-11-13	4478	4635	0	0	0	11-1998	---	
2006-11-13 to 2006-11-20	4408	4608	0	0	0	12-1998	16	
2006-11-20 to 2006-11-27	5030	4038	0	0	0	01-1999	1	
2006-11-27 to 2006-12-04	4247	4673	0	0	0	02-1999	6	
2006-12-04 to 2006-12-11	4168	4594	0	0	0	03-1999	3	
2006-12-11 to 2006-12-18	4068	5069	0	0	0	04-1999	7	
2006-12-18 to 2006-12-25	4179	4737	0	0	0	05-1999	10	
2006-12-25 to 2007-01-01	4725	4317	0	0	0	06-1999	8	
2007-01-01 to 2007-01-08	4906	4166	0	0	0	07-1999	4	
2007-01-08 to 2007-01-15	4635	4325	0	0	0	08-1999	5	
2007-01-15 to 2007-01-22	3892	5137	0	0	0	09-1999	15	
2007-01-22 to 2007-01-29	4632	4521	0	0	0	10-1999	12	

Value at Risk:

Infrastructure: 0 Processes; 0 Systems; 0 Categories.

Total N-Opvar: \$0K

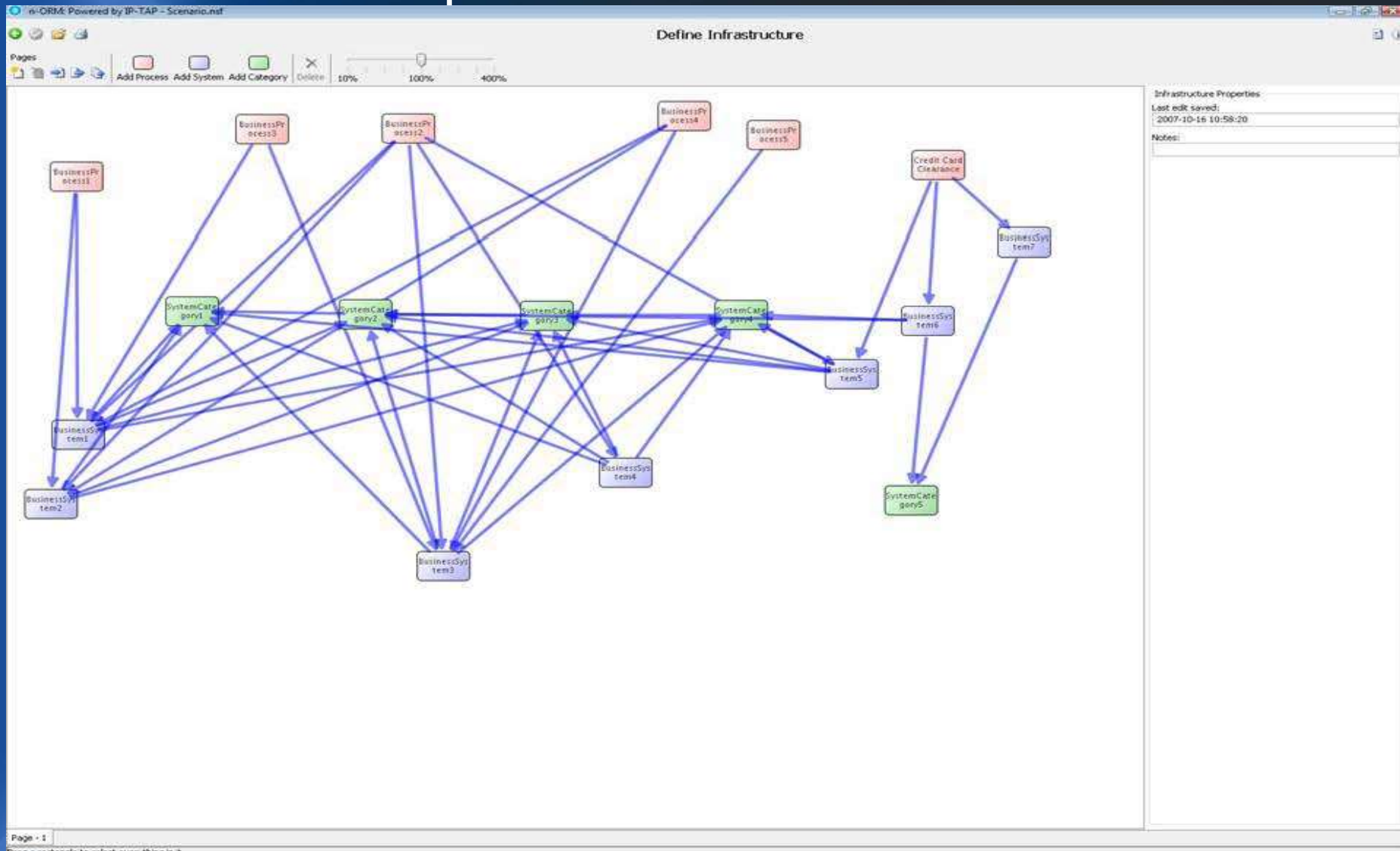
Key:

Observed	Externally-Sourced	User Input	Predicted
----------	--------------------	------------	-----------

Process Manager

- Processes, systems and categories are mapped in their relationships by internal personnel
- The output from the process manager is input into the main application
- Multiple instances of process manager can be given to individual workgroups, process managers etc
- Drag and drop functionality reduces training requirements to minutes.

Process Manager



Installation & Licence

- Back-end can be installed by internal personnel with network admin experience
- Can be installed by our personnel
- Can hold a centralized training day for internal personnel
- Can hold company-specific training per location if small number
- Control of use is controlled by Dongle under specific rights and obligations

Support Structure

- Product support via – NSC (front end) + LUEL (backend)
- Anticipate few requirements for support
- Debugging already undertaken with test site (1.25 years)
- Non-critical / non-real-time system
- Data confidentiality by all parties (only patterns IN the data, NOT viewable data content)
- NSC – military intelligence background i.e. high degree of confidentiality

Next Steps

Determine whether of interest to Swiss Re:

- a) as a product / service?
- b) as a system for its' own operations (FOC)?
- c) as a business case to provide cover for?
- d) as a distribution partner?
- e) as a JV development partner?