

---

# How to Manage Effectively Operational Risk

For  
Basel II, Solvency II and Arrow



---

## White Paper

September 2008

## Table of Contents

Loss Data.....	5
Risk and Control Self Assessment (RCSA).....	7
Key Risk Indicators.....	13
Action and Remediation Plans.....	15
Risk Simulation.....	16
Reporting.....	17
Key Benefits of Proposed Solution.....	18
About Dynasec.....	18

## Introduction

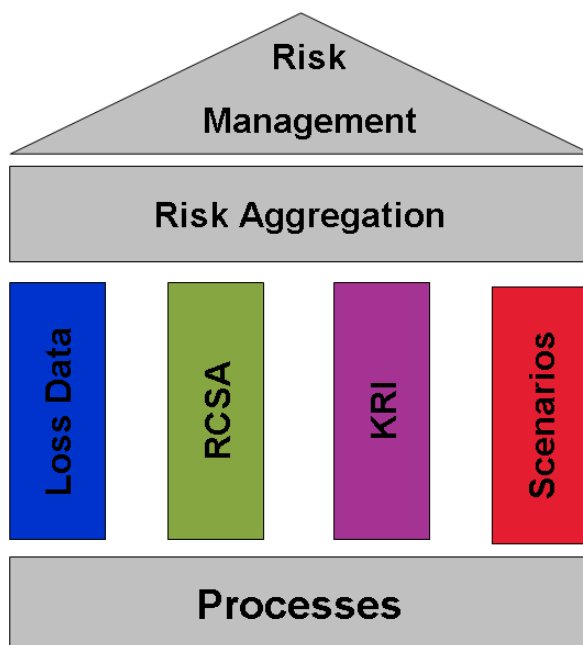
Operational risk exists everywhere in the business environment. It is the oldest risk facing any commercial institution and in particular banks, insurance companies and other financial institutions. Any financial institution will face operational risk long before it decides on its first market trade or credit transaction.

Of all the different types of risks financial institutions face, operational risk can be the most devastating and at the same time, the most difficult to anticipate. Its appearance can result in sudden and dramatic reductions in the value of a firm.

Operational risk cannot be managed successfully with a few spreadsheets or databases developed by an internal risk management department. In fact, one of the biggest mistakes an institution can make is to rely on simplistic and traditional solutions, which can lead to less than ideal choices about managing operational risk.

easy2comply™ enables organizations to efficiently meet and adapt to internal operational risk practices as well as external regulations such as: Basel II, Solvency II, FSA mandates and others by automating and simplifying the process of collecting, storing, analyzing, tracking and reporting on information relevant to operational losses, risk and control assessments, definition and management of key risk indicators and scenarios.

## easy2comply™ Operational Risk Architecture



## Loss Data

The loss database is a key, standard element of the Operational Risk Management module. The collection and analysis of internal loss data provides management information which can be fed back into the operational risk management and mitigation process. In addition, the database of internal loss events builds up over time and provides the basis for quantitative analysis and the calculation of capital allocation .

Data quality of loss reporting is often a major concern in many organizations. Dynasec Enterprise simplifies the collection of loss reporting by offering a 3-step process with built-in workflow capabilities:

### 1. Loss Event Capturing

In the first stage, authorized users can report on a loss event, a suspected loss event or a near miss. This loss event capturing process is performed with a comprehensive and customizable form that contains all the necessary fields and information for later loss event analysis.

### 2. Loss Event Evaluation

In the second stage, authorized users, generally from the risk management department, are automatically alerted of any loss event reported in the system. They can assess the impact of the loss event and describe the associated risks and damages in various formats which provide the basis for later in depth analysis and loss event reporting.

### 3. Loss Event Conclusions and Follow Up Actions

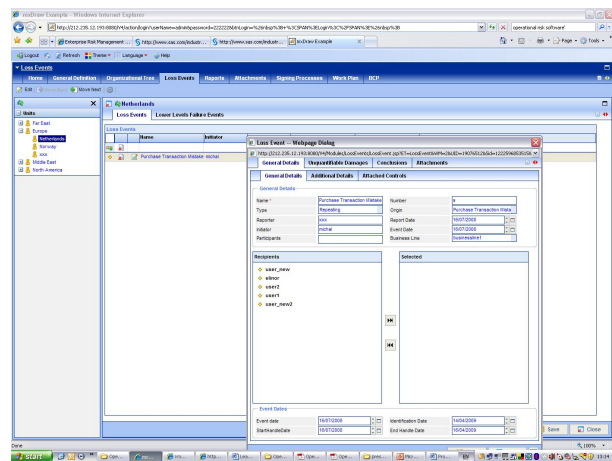
At this stage, authorized users can summarize the conclusions resulting from a loss event; define follow up action items with due dates, and assign responsible persons for each action item. All action items are incorporated

into easy2comply™'s integrated action and remediation plan for tracking and management of tasks.

easy2comply™'s flexible platform enables organizations to tailor their own fields in the loss database forms above, although certain standard fields such as selecting the appropriate Business Line and categorizing the Event Type are mandatory. Additional fields can easily be defined during the system configuration, requiring no programming.

**easy2comply™ offers the following standard fields:**

- Event Name
- Event ID
- Event Reporting Date
- Reporter Name
- Event Type (Internal/External)
- Related Organizational Unit
- Related Processes
- Related Business Line
- Related Event Category
- Related Controls
- First Event/Repeating Event/Near Miss
- Correlative Events (In case of a Repeating Event)
- Event Description
- Event Identification Day
- Start Handling Date
- End Handling Date
- Participants
- Key Personnel Involved
- Implemented Risks



- Implemented Risk - Direct Damage
- Implemented Risk - Indirect Damage
- Implemented Risk - Unquantifiable Damage
- Insurance Cover
- Conclusions
- Follow Up Action Task
- Follow Up Action Date
- Follow Up Action Responsible
- Attached Files
- Authorization process

## Risk and Control Self Assessment (RCSA)

Risk and Control Self Assessment (RCSA) is one of the integrated components that easy2comply™ offers for effective management of operational risk. easy2comply™ establishes a coherent structure that automates the entire workflow for managing the risk and control framework including: systematic documentation of processes and sub processes, identification of the risks that could prevent the attainment of process objectives and mapping of the controls that should be in place to mitigate these risks.

easy2comply™ is designed in a way that enables companies to construct both actual and 'horizontal' or virtual organizational structures for the operational risk management process. The flexible system provides up to 1024 layers of hierarchy in the organizational structure that can be defined by the system administrator. Furthermore, easy2comply™ enables the creation of an unlimited number of 'horizontal' or virtual organizational units which cross the actual organizational tree. Authorized users subjectively select single or groups of hierarchical organizational units within a horizontal unit. Such horizontal organizational units are used to identify cross- company trends and to perform competitive analysis between cross- company business units. (For example: all wholly-owned subsidiaries or all purchasing departments throughout the organization).

Organizational processes and sub-processes can be documented using an integrated flowchart engine which graphically represents the process flow. Each component in the flowchart is linked to the RCSA matrix, providing for easier documentation maintenance, consistency and improved change management.

Organizations who already document their structure in an external system can take advantage of easy2comply™'s open systems environment and import or link to pre-documented organizational trees.

Furthermore, processes are linked to organizational units using an m:n approach. This enables analyzing risk and controls from both perspectives: organizational and process-oriented.

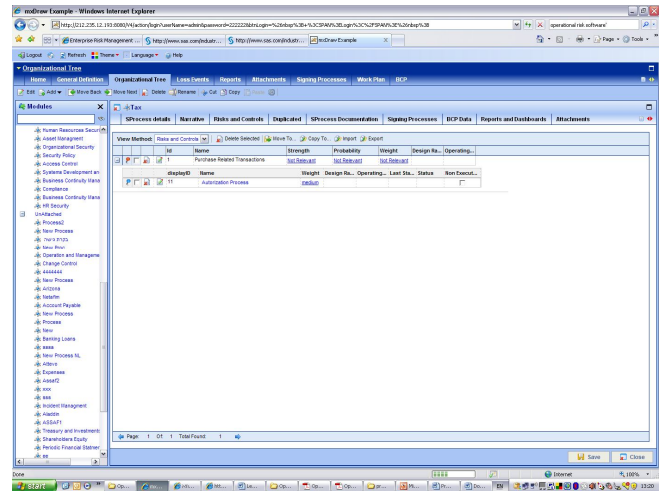
Risk Control Self Assessment can be performed at any level, including organizational units and processes. The self assessment can be based on data from 3 different sources: pre-populated data using a sophisticated templates mechanism, data built from scratch in the system during the assessment (and saved as a template if necessary) or legacy data previously accumulated and automatically inputted into the system. Adding, deleting and modifying information is easy and intuitive, although, subject to the user access rights that have been pre-selected.

Documenting and assessing risk both qualitatively and quantitatively includes but is not limited to the following information:

Risk Name

- Risk Description
  
- Qualitative Information (can be based on a risk assessment wizard)
  - Severity
  - Probability
  - Other

- Quantitative Information (can be based on a risk assessment wizard)
  - Severity
  - Probability
  
- Scenario Analysis
  - Normal Scenario
    - Description
    - Loss
    - Frequency
    - More...
  - Serious Case Scenario
    - Description
    - Loss
    - Frequency
    - More...
  - Disaster Scenario
    - Description
    - Loss
    - Frequency
    - More...
  
- Risk Category
- KRI
- Key Risk
- Risk Type
- Tolerance Level
- Risk Response



Documenting and assessing controls includes but is not limited to the following information:

- Control ID
- Control Activity Description
- Control Objective
- Control Activity In Place
- Control Weight
- Key Control
- Control in Place
- Control Design Rating
- Control Owner
- Control Nature
- Control Frequency
- Relation to COSO
- Financial Effect
- Preventive/Detective
- Recommended Testing Procedure
- Sample Size Required
- Criteria for Effectiveness Testing
- Criteria for Ineffectiveness Testing
- Tester
- Testing Start Date
- Testing Due Date
- Attachment
- Findings
- Recommendation
- KPI
- Attachments
- On Management Procedures

The relations between risks and controls is based on an m:n approach where each risk can be mitigated by several controls and every control can impact various risks.

The system also allows for a correlation of m:n between controls. easy2comply™ allows for control hierarchies and dependencies between controls. For example, a control status can be based on a calculation of sub-controls. Each control in the system might have a different index of status which can be defined by the authorized users.

easy2comply™ provides functionality for copying, importing and exporting risk and controls between different segments of the organization tree and/or the process tree and can define multiple types of relations between them. Throughout the lifecycle of the operational risk management process, the system enables the reduction of the overall number of risks and controls being managed in the organization which results in a more efficient operation.

## Key Risk Indicators

Key Risk Indicators (KRI) allocation and analysis is a core feature of Dynasec Enterprise Operational Risk module. The KRI module provides management with an early-warning system, underscoring those areas where pre-defined thresholds are exceeded and thus highlighting potential danger spots in a timely fashion.

Each Key Risk Indicator can be automatically generated or manually entered. Dynasec Enterprise provides the infrastructure to develop and determine both of these methods. KRIs are freely definable and there is (practically) no limit to the number or type of KRIs which can be set up.

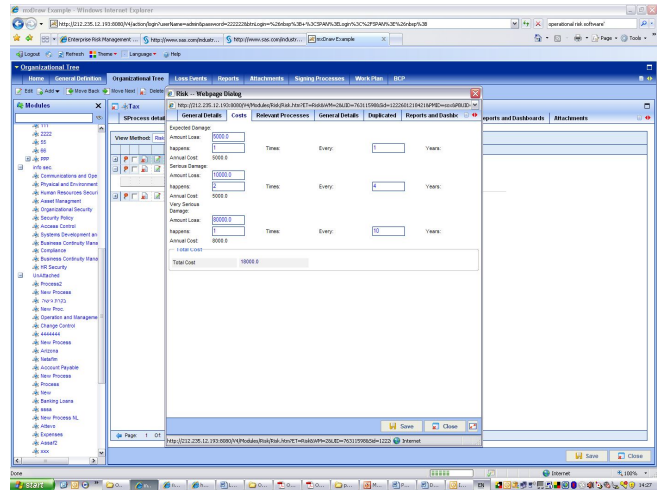
Some of the basic information for an automatic KRI is held within the Dynasec Enterprise system. In fact, the information can be embedded in the risk control self assessment process as for example, a KRI when there are a number of missing controls in a process. Organizations can take advantage of this integrated approach to reduce the time required for reconciliation or other cross-checking requirements.

Alternatively, if the required information is located in external, typically transaction-based systems, easy2comply™ can link to those systems via standardized protocols to gather the required information. For example: the number of dealer transactions rejected for exceeding trading limits can be a KRI created and tracked in the system which has been linked to the external application that manages dealer transactions and calculates this figure.

There are situations where the information is more readily available manually or where it is not found in any other system. In these cases, suitably authorized managers can enter the KRI values directly into the system, online.

Documenting and assessing KRI's includes but is not limited to the following information:

- KRI ID
- KRI Name
- KRI Description
- KRI Type (KRI, KCI, KPI)
- KRI Source
- KRI Norm
- Related Risk(s)
- KRI period
- KRI Test
- KRI Impact
- KRI Change
- Correlated KPI/KCI
- Conclusion
- Action Plan
- Other



## Action and Remediation Plans

easy2comply™ provides integrated risk measure/action plan functionality in the operational risk management module. This functionality enables creation, execution, management and follow-up of action and remediation plans in order to improve organizational processes and controls and to mitigate risk exposure.

Action plans can be defined by authorized users as a result of:

- Poor Control
- Loss Event
- KRI
- Simulation
- Other general events

:

Each action plan includes but is not limited to the following information:

- Task Owner
- Due Date
- Task Description
- Related Organizational Units/Processes/Risks/Controls
- Task Status
- Authorization Process
- Log of Authorized Changes
- Log of Rejected Changes
- More

Open tasks can be distributed to the owners. An email will be automatically sent by the system to notify each owner of his or her tasks with a link to the system. A reminder will be sent if the task date has passed and escalation alerts and procedures can be defined to enable additional emails to be sent to selected managers or other individuals.

## Risk Simulation

Risk simulation is an integral feature of the easy2comply™ Operational Risk module. A typical operational risk framework in many organizations includes several sources of information such as internal and external loss data, risk and control self assessment and key risk indicators. The Risk Simulations enable the analysis of this information by creating correlations between the different sources of information using various mathematical and statistical methods.

easy2comply™ Risk Simulation includes, but not limited to, the following information:

- Organizational Loss Distribution Approach
  - Severity
  - Probability
  - Periodic (Annual, 3 years, 5 years)
- Various vertical and horizontal angles of analyzing LDA:
  - Per Business Unit
  - Per Business Line
  - Per Process
  - Per Category Type
  - Per Horizontal Units
- Value at Risk Calculations using :
  - Monte Carlo Simulation
  - Historical Simulation (in development)
  - Variance - Covariance Matrix (in development)
- Residual Risk Distribution
- Control Status Analysis
- Heat Maps
- Horizontal Risk and Control Analysis
- More

## Reporting

easy2comply™ provides management reporting tools for both regular and ad-hoc reporting requirements including dashboards, pre-built, standardized reports and a user-friendly report generator. The outputs generated by the different reporting options can also be exported to external tools such as Excel, PDF, Power Point and Word and allow the organization to identify trends and to perform analysis from multiple perspectives as outlined below.

The Operational Risk Management Module supports multiple building blocks including:

- Organizational Units
- Processes
- Risks
- Controls
- Loss Data
- KRIs
- Simulations
- IT Systems
- Business Lines
- Risk Categories
- People



In easy2comply™, each building block can serve as a basis for analyzing the information and aggregating the data. You can view graphic dashboards with drill-down capabilities and run both textual and graphical reports, such as pie charts and distribution schemes.

easy2comply™ Report Generator enables authorized users to define on their own report templates and re-use these templates at any time or in conjunction with any building block. When building a report template, all data base fields are available for selection and can serve as a basis to filter the information when running the report.

## Key Benefits of Proposed Solution

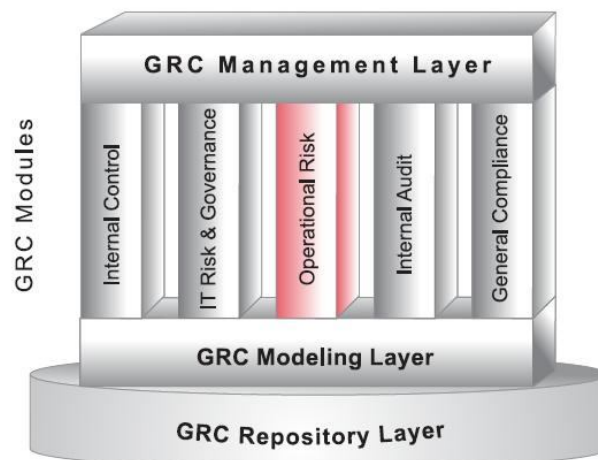
The main benefits an organization can enjoy from deploying easy2comply™ Operational Risk Management modules are:

- ✓ Increase accuracy and visibility of your risk information
- ✓ More quickly identify and remediate deficiencies
- ✓ Increased management insight
- ✓ Optimization of business performance
- ✓ Reduce the cost and complexity of your operational risk process
- ✓ Integration of all risk management components on a single, coherent platform
- ✓ Incorporate a robust software architecture to incorporate current and future operational risk management needs

## About easy2comply™

easy2comply™ software platform is composed of 5 solution families:

- Operational Risk Management
- Internal Control Management - including SOX, MiFID, Turnbull, JSOX, etc.
- IT Risk and Governance - including CobiT, ISO27001/17799, BCP, BCM, ITIL, etc.
- Internal Audit Management module
- General Compliance Framework - a toolkit for customization to specific governance and compliance needs (eg. LOPD, etc.)



**About Dynasec**

Dynasec Ltd. is a leading provider of Governance, Risk Management and Compliance (GRC) solutions. Our flagship product, easy2comply™ is the perfect answer for businesses of all sizes seeking to simplify their compliance and risk management processes.

easy2comply™ can be deployed either on-demand (SaaS) or on-site to suit each customer's preferred configuration. We serve customers in many markets including: financial institutions, telecom, energy, and government, pharmaceutical, healthcare, commercial organizations.

Dynasec's customers include financial institutions, telecom, energy and other many other enterprises. The Dynasec customer base includes:

**Financial Sector**

- Rabobank
- Generali (Migdal)
- Mitsui Sumitomo Insurance
- Dexia
- Prisma Financial Services
- Mastercard Israel
- Phoenix Insurance
- Bank Igud
- Leumi Group
- Bank Hapoalim
- First International Bank of Israel
- United Mizrahi-Tfahot Bank

**Government, Energy, Telco, Other Sectors**

- Dutch Ministry of Social Services
- Israel Electricity Company
- Ormat Thermal Power
- Israel Water Authority
- Clalit Health Services
- Cellcom
- Blue Square retail
- Gilat Satellites
- Ministry of Finance, Division of Capital Markets, Insurance, Savings
- Zim Shipping Lines
- Netafim Drip Irrigation

easy2comply™ - Practical Compliance Solutions

affordable. reliable. easy2deploy.

[www.easy2comply.com](http://www.easy2comply.com)

