ENTERPRISE RISK MANAGEMENT

Enterprise Risk Management (ERM) in an organization includes the business processes and methods used to identify and manage risks as well as seize upside opportunities to achieve its objectives. ERM, therefore, provides a methodological framework in risk management for identifying risky events or conditions relevant to the organization's objectives, risks, and opportunities, identifying and assessing these conditions in terms of *Likelihood* or frequency of occurrence as well as the risk condition's magnitude of *Impact*, determining risk mitigation and postrisk response strategy, and monitoring the progress of these risk controls. When organizations identify and proactively address risks and opportunities, organizations are able to protect and create value for their stakeholders (e.g., owners, employees, shareholders, executives, customers, regulators, nations, and society in general).

ERM is usually also described as a risk-based approach to strategic planning as well as for managing an organization by integrating internal risk controls and external risk-compliance requirements (e.g., COSO, ISO 31000:2009, Basel III, and Sarbanes–Oxley Act). It applies to a broad spectrum of risks facing an organization to ensure that these risks are properly identified and managed. Investors, government regulators, banks, and debt rating agencies, among others, tend to scrutinize the risk-management processes of an organization as a key metric to its potential success.

In addition, the reasons for an organization to implement ERM should, at the very least, include the following areas of concern:

- Alignment of Risk Appetite and Strategy. Senior management typically considers the organization's risk appetite when strategic investment alternatives are being evaluated, as well as when setting objectives and developing mechanisms to manage risks. This tactic helps the organization to align its risk objectives with its business processes.
- Enhanced Risk-Response Decisions. ERM provides both the qualitative and quantitative rigor to identify and select from among alternative risk responses, including strategic real options and analysis of alternatives for risk avoidance, risk reduction, risk sharing, risk mitigation, and risk acceptance.
- Reduction in Operational Surprises and Losses. Organizations will gain enhanced capabilities to Identify, Assess, Prioritize, Value, Diversify, and Mitigate potential risk events' losses using advanced quantitative risk analytics. Instead of just qualitatively identifying risks, organizations can now translate these qualitative elements into quantitative risk models where Monte Carlo Risk Simulations, Stochastic Modeling, Portfolio Optimization, Predictive Forecasting, Business Intelligence, and Capital Investment Valuation and Modeling can be performed.
- Identify and Manage Multiple Cross-Enterprise Correlated Risks within a Corporate Portfolio Environment. Every enterprise faces a myriad of risks affecting different parts of the organization. ERM facilitates effective response to these interrelated and correlated impacts and integrates responses to multiple risks. Financial risks and risks in capital investment projects can also be handled within the environment of a correlated portfolio of projects where risks are hedged and diversified.
- Seizing Opportunities. Risks imply uncertainties, and uncertainties carry with them downside risks as well as upside potential. By considering a full range of potential events and risks, and

creating Strategic Investment Flexibility or Strategic Real Options, management will be positioned to proactively realize upside opportunities, while at the same time mitigate downside risks.

- Improved Capital Deployment. Robust Quantitative Risk Metrics and Key Performance Indicators (KPI) generated through a comprehensive ERM process will allow management to effectively assess overall capital needs and enhance its capital allocation (e.g., creating an Efficient Investment Portfolio subject to Budgetary, Schedule, Strategic, and other Constraints).

The Typical Traditional ERM Process

Traditionally, the ERM process involves *qualitative* risk assessment and documentation. The following lists the standard approach and traditional ERM process, which of course, can be modified and adapted to fit the organization under analysis. Throughout the rest of the whitepaper, we will revisit some of these steps to incorporate Integrated Risk Management (IRM)® methods and overlay *quantitative* risk management techniques onto the process.

- Establish senior management buy-in and risk-management culture.
- Seek the board of directors and senior management involvement and oversight to discuss a risk-management framework and its benefits and to obtain agreement on high-level objectives and expectations with resources and target dates regarding risk management in line with the organization's strategic plan.
- Review existing ERM practices in the organization and identify areas for improvement.
- Facilitate initial training and working sessions to ensure buy-in and establish risk-management culture with key personnel involved with ERM implementation.
- Conduct working group discussions with stakeholders and key personnel to identify sources of risks.
- Provide input for implementation in the strategic business planning process.
- Coordinate the development, implementation, and monitoring of identified risk metrics.
- Document risk inventories and mitigations within Risk Registers in the organization.
- Develop risk dashboards for presentation to senior decision makers and the board of directors.
- Assess exposure to the risk, assess adequacy of existing risk mitigation or monitoring, and identify opportunities to enhance mitigation or monitoring activities, then suggest and build best practices for enhanced risk-adjusted returns.
- Create reports that effectively and concisely deliver the business intelligence based on risk measures that management needs to make cost-effective financial decisions.
- Establish a reporting process for management and the board.
- Establish a management working group to support the resources identified and drive the effort across the organization.

Risk Registers and Basic Enterprise Risk Management

The typical traditional ERM method uses *Risk Registers*, which simply involves recording all risks present or anticipated. Each *Risk Element* (i.e., each risk item that is recorded in the Risk Register) may include information on the name of the risk, the category or type of the risk, who reported it, who is responsible or is assigned the risk, what if any risk mitigation or risk control is required, contact person, documentation, and so forth. Sometimes additional information such as frequency, or *Likelihood,* and severity, or *Impact* that risk may have on the organization is included. These Likelihood and Impact measures are usually qualitative estimates (high, medium, low) or can be assigned numerical values (1 to 5 or 1 to 10, where the higher the frequency or severity, the higher the value assigned). Alternate methods

of using Vulnerability (or the inverse of amount of risk mitigation completed) with multiple risk controls are also supported. Clearly the amount of information and detail required varies depending on the organization. One way to think of Risk Registers is akin to a check register. For example, if you have a checking account, you can write a check to pay a specific bill; on that single check, you write the recipient's name, date, and amount. You can, of course, write multiple checks to different recipients. And every time a check is written, you would record said checks in a check register (whether electronically in an accounting software or manually in a physical check register). Continuing with this analogy, each check represents a different risk element, and multiple risk elements make up the Risk Register. You may also own multiple bank accounts, each with its own check register, or, in other words, an organization may have multiple Risk Registers set up, one for each division or business unit or project, and so forth.

However, the use of only Risk Registers by themselves often leads to ritualistic decision making, an illusion of control, and the fallacy of misplaced concreteness and reliance on purely qualitative risks. While the use of Risk Registers is a good starting point, Integrated Risk Management takes this qualitative assessment to the next level with more powerful quantitative risk management approaches.

Case Example: Hospital Risk Management

A simple example of a Risk Register in a hospital is shown in Figure 1, where certain types of risk events (e.g., wrong dosage given, equipment failure, etc.) that have occurred within specific departments (e.g., surgery, intensive care) and the number of events that happened within a specific time period are recorded, as well as other qualitative notes and associated details. Reports are then typically generated. Figure 2 shows a sample periodic (e.g., monthly) report of another organization showing the number of risk events that occurred in the past.

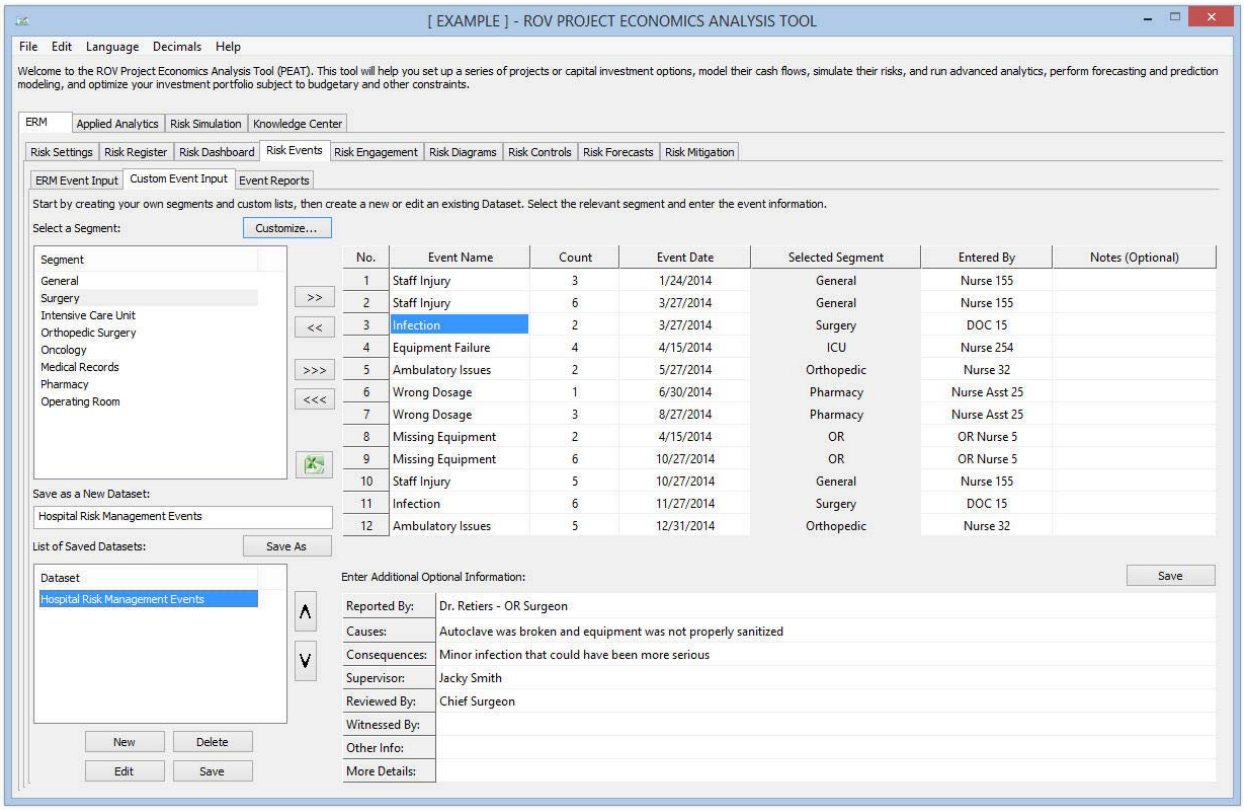


FIGURE 1 Example risk events in a hospital.

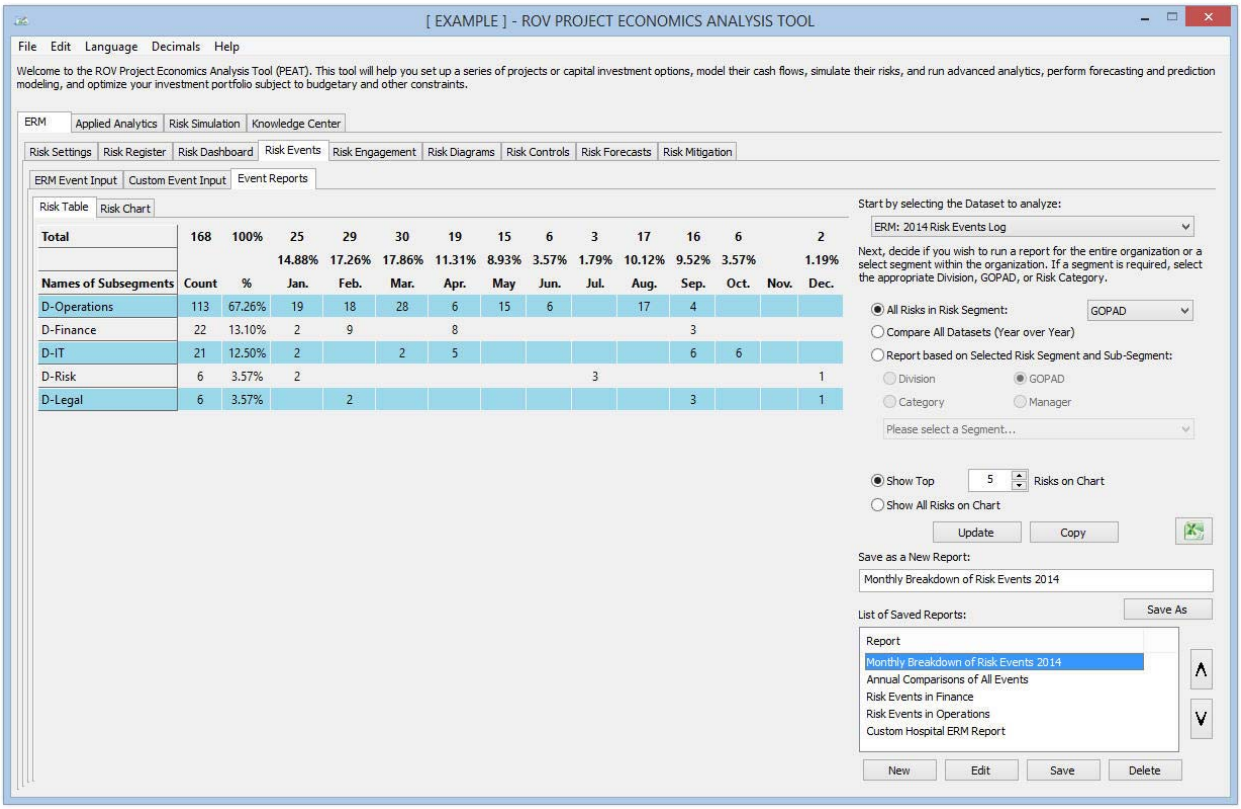


FIGURE 2 Example risk event reports.

Risk Matrixes

In other types of Risk Registers, *Likelihood* (*L*) and *Impact* (*I*) values can be used and entered for each risk element, and the product of these two variables is termed the *Key Risk Indicator* (*KRI*), where $KRI = L \times I$. These KRI values can be color coded into various regions based on their respective values. For instance, Figure 3 shows a 10 × 10 matrix where the columns going from left to right represent Likelihood from 1 to 10 (low to high), and the rows from bottom to top represent the Impact from 1 to 10 (low to high). The values inside each of the cells represent the KRI, and the color coding depends on the computed KRI (typically, lower KRI values are green, medium KRI values are yellow, and high KRI values are red). In a later section, we showcase examples of how these KRI values can be incorporated into the ERM Risk Register. As will be seen later, the color coding, matrix size, and category labels can be customized as required.

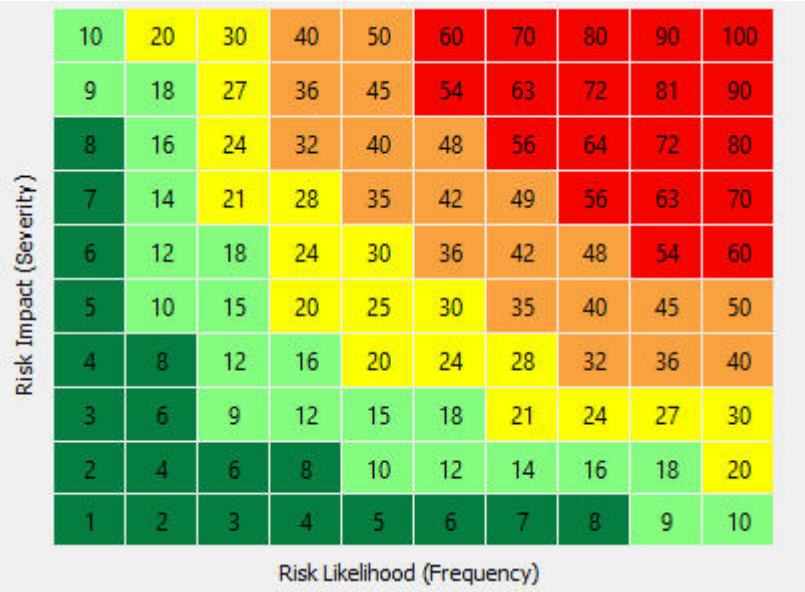


FIGURE 3 Risk matrix.

Business Continuity Planning

In some organizations with potential public risk exposures—such as nuclear power plants, airline companies, oil and gas exploration and drilling firms, banks, and government or public institutions—additional risk documentation is also recommended. These documentations are also part of the traditional ERM process. As an example, the following are typical procedures and documentation arising from operational risk planning, and they can be customized to an organization's unique needs:

- **Business Continuity Plan (BCP)** focuses on sustaining business functions during and after a disruption (e.g., business functions may include an organization's payroll process or consumer information process). A BCP may be written for a specific business process or may address all key business processes. IT systems are considered in the BCP in terms of their support to the business processes. A Disaster Recovery Plan, Business Resumption Plan, and Occupant Emergency Plan may be appended to the BCP as required.
- **Business Recovery Plan (BRP)** or **Business Resumption Plan** addresses the restoration of business processes after an emergency. Development of the BRP will be coordinated with the Disaster Recovery Plan and BCP.
- **Continuity of Operations Plan (COOP)** focuses on restoring an organization's main essential functions at an alternate site and performing those functions for up to 4 weeks before returning to normal operations. COOP addresses headquarters-level issues; it is developed and executed independently from the BCP. The document can include Delegation of Authority, Orders of Succession, and Procedures for Vital Records and Databases.
- **Continuity of Support Plan** and **IT Contingency Plan (Recovery Strategy)** includes the development and maintenance of continuity of support plans for general support systems and contingency plans for major applications.
- **Cyber Incident Response Plan (CIRP)** establishes procedures to address cyber-attacks against an organization's IT system. It is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data,

denial of service, or unauthorized changes to system hardware, software, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse).

- **Disaster Recovery Plan (DRP)** becomes applicable after catastrophic events that deny access to the normal facility for an extended period. Depending on the organization's needs, several DRPs may be appended to the BCP.
- **Crisis Management Plan (CMP)** and **Crisis Communications Plan (CCP)** detail how organizations prepare their internal and external procedures prior to and during a disaster. A crisis communications plan is often developed by the organization responsible for public outreach. Plan procedures are included as an appendix to the BCP. The communications plan includes designation of specific individuals as the only authority for answering questions from the public regarding disaster response.

Comprehensive ERM with Quantitative Risk Management

A true next-generation comprehensive ERM process should include, at a minimum, the qualitative methods and steps previously outlined plus quantitative IRM methodologies. Instead of continuing the whitepaper by outlining additional items and bullet lists of methods and steps, we illustrate the quantitative ERM methods through the use of the PEAT software.

PEAT: Project Economics Analysis Tool

Project Economics Analysis Tool (PEAT) software was developed to perform a comprehensive Integrated Risk Management analysis on capital investments, discounted cash flow, cost and schedule risk project management, oil and gas applications, healthcare analytics, and Enterprise Risk Management. This tool will help you to set up a series of projects or capital investment options, model their cash flows, simulate their risks, run advanced risk simulations, perform business intelligence analytics, run forecasting and prediction modeling, optimize your investment portfolio subject to budgetary and other resource and qualitative constraints, and generate automated reports and charts, all within a single easy-to-use integrated software suite. The following modules are available in PEAT (Figure 4), and this whitepaper focuses on the ERM module:

- Enterprise Risk Management (ERM)
- Corporate Investments (Dynamic Discounted Cash Flow)
- Corporate Investments (Lease versus Buy)
- Goals Analytics (Sales Force Automation)
- Healthcare Economics (HEAT and REJ)
- Oil and Gas (Oil Field Reserves, Oil Recovery Analysis, Well-Type Curves)
- Project Management (Cost and Schedule Risk)
- Public Sector Analysis (Knowledge Value Added)
- ROV Compiled Models
- Customized company-specific modules and applications

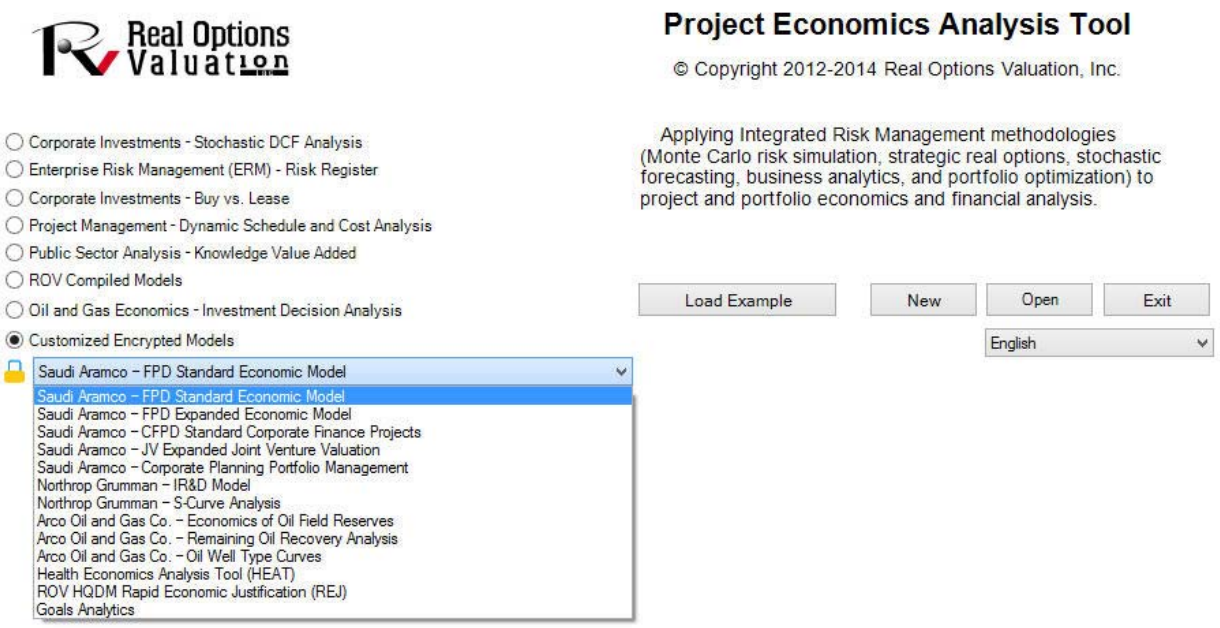


FIGURE 4 Project Economics Analysis Tool (PEAT) by ROV.

ROV's PEAT incorporates all of the advanced risk and decision analytical methodologies covered in the Integrated Risk Management (IRM) process into a simple-to-use and step-by-step integrated software application suite. It simplifies the risk-based decision analysis process and empowers the decision maker with insights from powerful analytics. If you already perform discounted cash flow modeling or Enterprise Risk Management in Excel, why do you still need PEAT? Because PEAT's integrated advanced analytical techniques extend the analysis you have already performed, and do so in a simple-to-use, simple-to-understand, and automated format, thus generating valuable insights that would be impossible without such advanced methods. PEAT allows you to scale and replicate your analysis, archive and encrypt your models and data, create automated reports, and customize your own PEAT modules.

- *Enterprise Risk Management (ERM)*: Perform traditional qualitative ERM with Risk Registers but also enhance the analysis with more quantitative analysis. This ERM module comes with an online Web version as well as a module within PEAT, where you can enter and save multiple Risk Registers to generate Key Risk Indicators (KRI) by Risk Divisions and Risk Taxonomy (Geographic, Operations, Products, Activity or Process, and Department); assign risk items to different Risk Managers by performing Risk Mapping of Risk Categories to different Risk Divisions; create Risk Dashboards of the results; enter Risk Elements within multiple customizable Risk Engagements; draw Risk Diagrams; perform and run Risk Controls on KRIs to see if certain risks are within control or out of control; perform Risk Forecasts; check if certain Risk Mitigation projects do, indeed, work or are statistically ineffective; perform Risk Sensitivity on KRIs; perform Risk Scenarios on quantitative risk metrics; run Risk Simulations on risk metrics; generate Risk Reports; and encrypt your data and files for the purposes of Risk Security. See Dr Johnathan Mun's Modeling Risk, Third Edition, Chapter 14, for the case study on Eletrobrás in Brazil on how The PEAT ERM was employed at this multinational.
- *Corporate Investments (Dynamic Discounted Cash Flow)*: With a few simple assumptions, you can auto-generate cash flow statements of multiple projects; obtain key performance

indicators and financial metrics (NPV, IRR, MIRR, PP, DPP, ROI); run risk simulations on uncertainty inputs; generate static Tornado sensitivity analysis; run dynamic sensitivities; simultaneously compare multiple projects within a portfolio; perform forecasts of future revenues and cash flow; draw multiple strategic investment pathways and options, and model and value these strategic paths; compute and optimize the best projects within a portfolio subject to multiple constraints and restrictions; view results in management dashboards; encrypt your model and data; and auto-generate analysis reports. See Dr. Mun's Modeling Risk, Third Edition, Chapter 18, for more details on using PEAT's stochastic discounted cash flow module.

- *Corporate Investments (Lease versus Buy)*: Run a lease versus buy analysis, compare capital and operating leases with interest payments and tax advantages, value the lease contract from the point of view of the lessee and lessor, and generate the complete cash flow analysis to obtain the net advantage to leasing.
- *Goals Analytics (Sales Force Automation)*: Develop and maintain corporate sales goals. A Web-based SaaS and desktop-based PEAT module, it focuses on the creation and use of goals that help make goal-setting more accurate and sustainable by any company seeking to improve its sales performance (sales goal forecasting, probability of hitting corporate revenues, sales pipeline analysis, and other sales-based metrics analysis). See Dr. Mun's Modeling Risk, Third Edition, Chapter 14, for a case study on using PEAT's business plan forecasting module.
- *Healthcare Economics (HEAT and REJ)*: Run the economics of various options available under the U.S. Affordable Care Act (Obamacare) for corporations providing employer-sponsored healthcare by loading employee-census data (healthcare economics analysis tool, HEAT), or perform rapid economic justification (REJ) of each option by simulating its high-level inputs. See Dr. Mun's Modeling Risk, Third Edition, Chapter 14, for a case study on using PEAT's health care economics module.
- *Oil and Gas (Oil Field Reserves, Oil Recovery, and Well-Type Curves)*: Perform oil and gas industry models on analyzing the economics of oil field reserves and available oil recovery based on uncertainty and risks, as well as generate oil-well–specific type curves and economics.
- *Project Management (Cost and Schedule Risk)*: Draw your own project pathways (simple linear project tasks versus complex parallel and recombining projects), then click a button to auto-generate the model. Enter the cost and schedule estimates as well as their spreads, then run a risk simulation on the model to determine the probability of cost-schedule overruns, cost-schedule buffers at various probabilities of completion, critical path identification, and sensitivity analysis. See Dr. Mun's Modeling Risk, Third Edition, Technical Note 6, for a case study on using PEAT's project management (cost and schedule risk) module.
- *Public Sector Analysis (Knowledge Value Added)*: Model government and nonprofit organizations' value, value to society, or intangible value via Knowledge Value Added utilizing market comparables to identify and monetize such projects and assets.
- *ROV Compiled Models*: With the compiler software, users can compile their existing Excel models into license-controlled executable EXE files. ROV's patented methods can be used to encrypt and lock up the intellectual property and mathematical algorithms of the model, and issue hardware-controlled and timed licenses to the purchaser's own users or customers.

Critical ERM Risk Characteristics and Modeling Criteria

PEAT ERM is both a desktop software and online Web-based application, with over 20 related U.S. and worldwide patents and patents pending. The desktop PEAT version is for internal risk department personnel to manage the results and data set, keep the data encrypted and safe, and run analyses such as simulations, scenarios, Tornado analysis, and so forth. Not everyone needs these advanced analytics. Therefore, in a large corporation, there can be multiple end users who should have the ability to enter data, and a few local administrators with access to control everything from granting access to and creating end users, to setting up the risk profile of the company. End users (e.g., plant managers, supervisors, secretaries, etc.) can only enter in data and information. These end users have limited access and limited knowledge, making training simple, and they enter in values only pertaining to their areas of responsibilities. Local administrators then have a database that rolls up to the corporate level and they can see results, generate reports, perform more advanced quantitative risk analytics, and so on.

- ### Risk Settings and Risk Classifications

Users typically start by setting up how Key Risk Indicators (KRI) should be set up, any E-Alerts that need to be triggered and sent if KRIs exceed certain values for any Risk Element, etc. Such global settings should also allow users to set Risk Indicator Categories (1-5 or 1-10) with Customizable Color Coding of KRI (Key Risk Indicators) via a Risk Matrix (Figure 5).

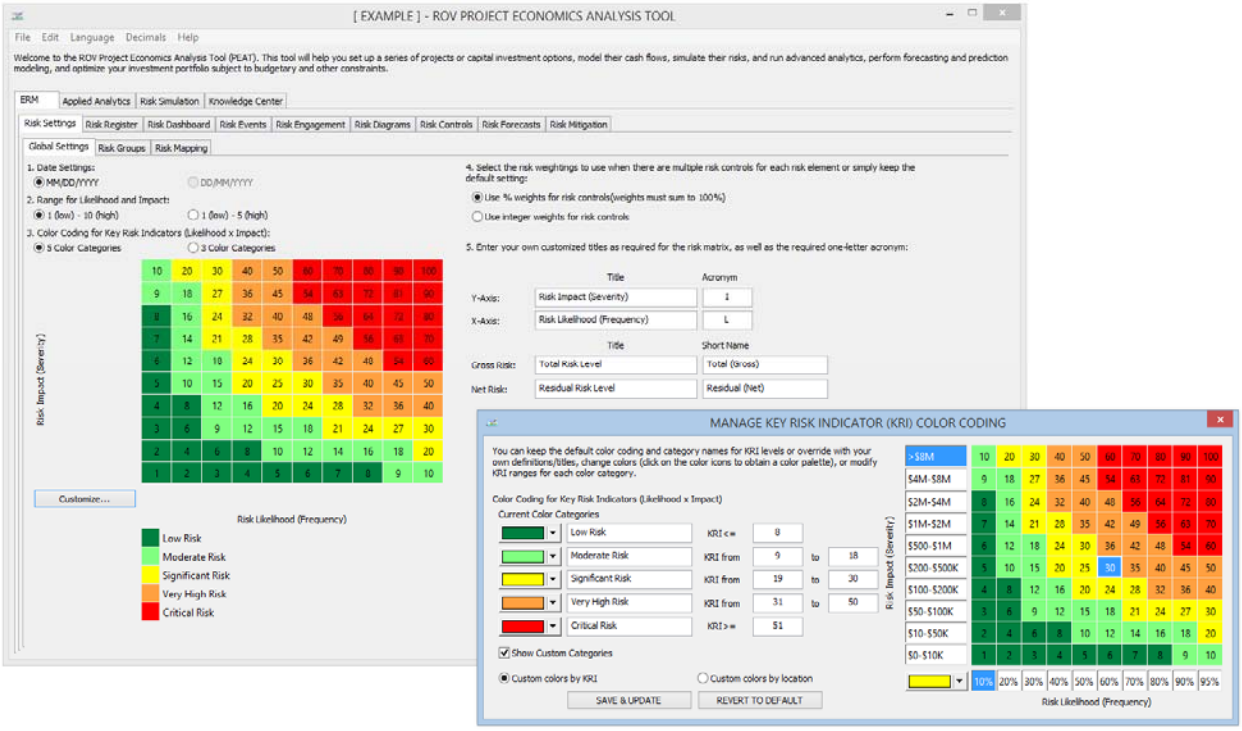


FIGURE 5 Risk settings.

- ### Risk Groups and Risk Taxonomy

Typically, ERM implementation also requires the ability to create various divisions, departments, risk categories, and other segmentation within an organization. Such segregation is required because data entered for the Risk Elements can be sliced and diced every which way, as well as being in compliance with COSO Integrated Risk Framework.

Figure 6 shows the PEAT set up of various Risk Divisions, Risk G.O.P.A.D., Risk Category, and Risk Managers. Cumulatively, these categories represent the Risk Taxonomy of the ERM system. For example, multiple business or operational Divisions within a Company can be created, such that the company can manage multiple risk profiles for each division. Users can also create and assign various G.O.P.A.D. categories (geographic, operations, products, activity or process, and department) such that analysts can analyze the company's risk profile from multiple points of view, select from and create queries of specific G.O.P.A.D. categories to analyze, and so on. Users can create customized Risk Categories or use PEAT's library of predefined risk categories, and lists of persons in charge of certain risks and their contact information can be set up.

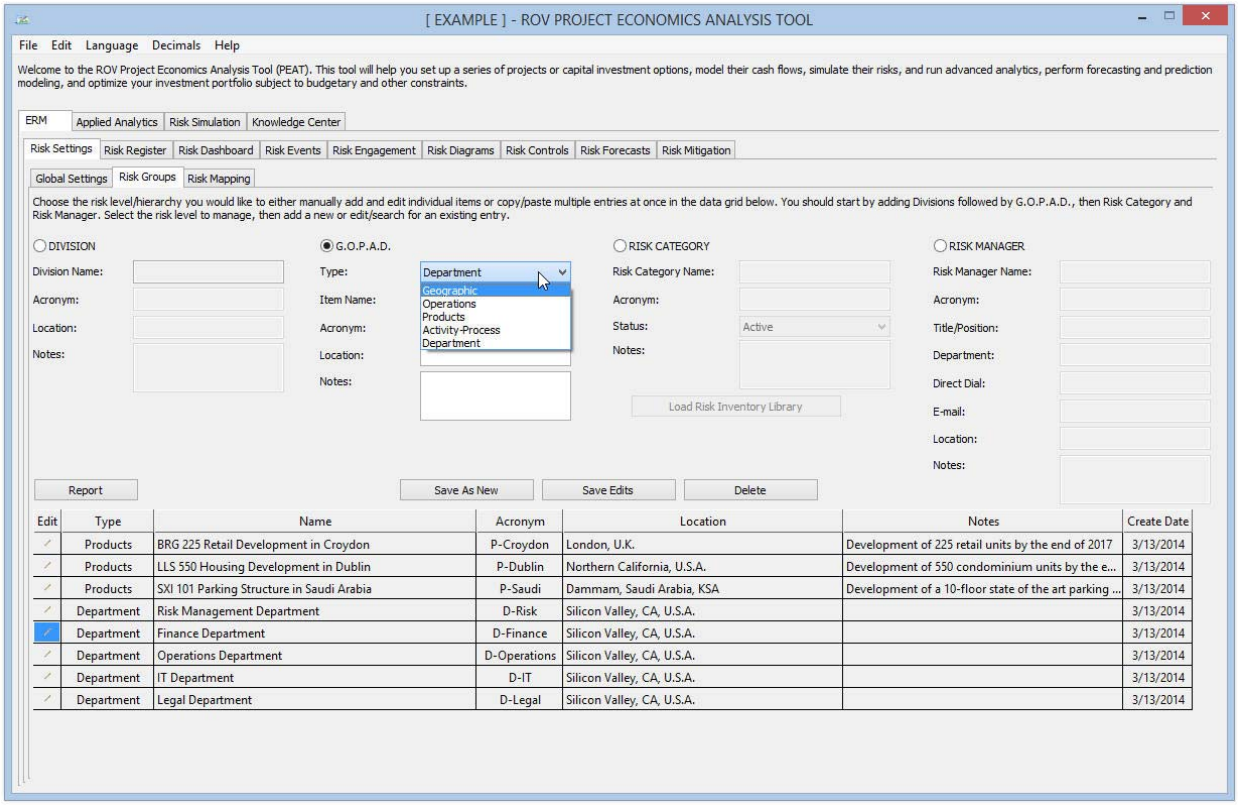


FIGURE 6 Risk groupings in an organization.

- **Risk Mapping**

Based on previously created Risk Groups and Risk Taxonomy, we can now map and link these hierarchies on one or more dimensions. This process will allow putting various projects with related risks into the various groups and segments for analysis and the ability to view how a certain risk permeates through the organization as well as how a specific risk element may touch multiple departments, divisions, processes, and so forth. The previously completed segments can then be mapped as shown in Figure 7. For example, a Risk Category can be mapped to one or multiple G.O.P.A.D. categories, which can then be mapped to one or more Divisions. All Divisions roll up to the Corporation. This way, when a risk element is entered in the Risk Register, users can choose the Risk Category and the remaining connection routes will be determined. Using these mapped connections, the software can slice-and-dice and look at different Divisions, G.O.P.A.D. categories, or Divisions and see the risk profile from various points of view.

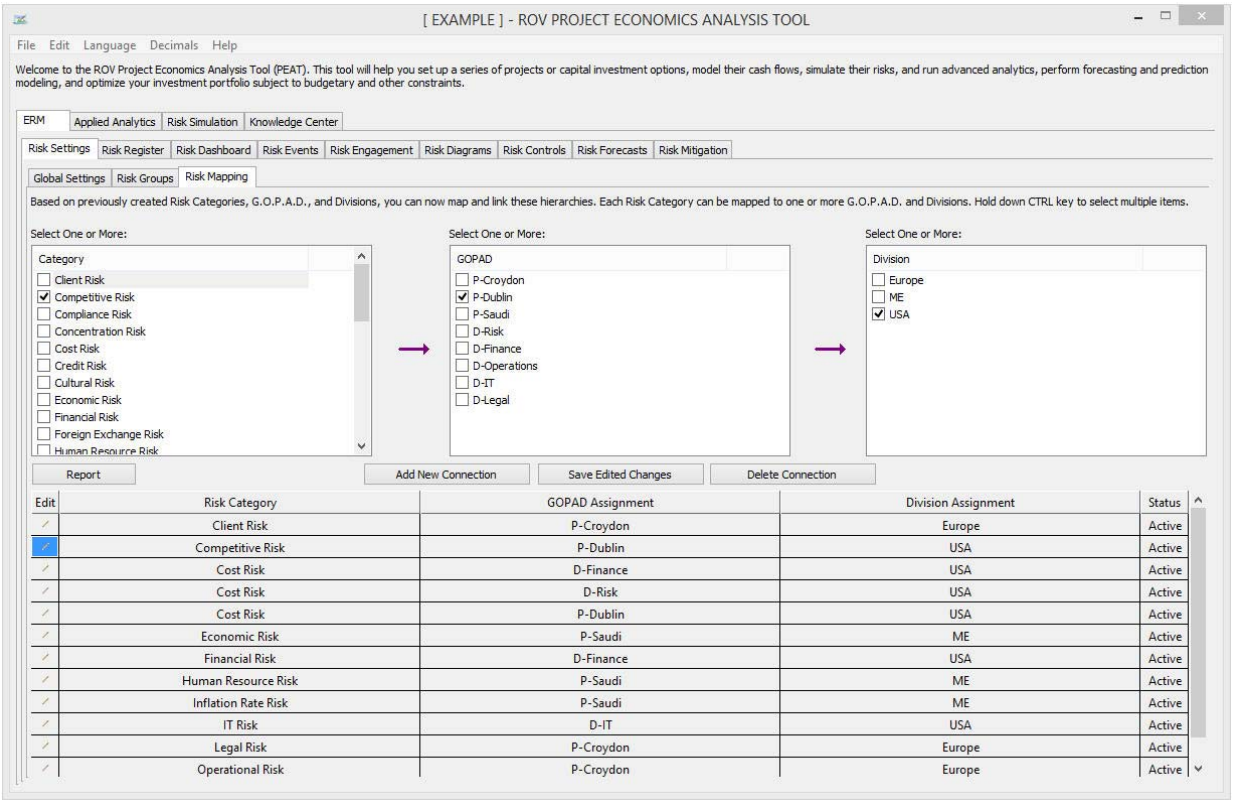


FIGURE 7 Risk mapping or grouped relationships.

- **Risk Register**

Now comes the Risk Register setup. As discussed, the Risk Register represents the center of the ERM world, and in the PEAT utility, users can set up, create new, and save multiple Risk Registers in a single file. That is, users can create multiple Risk Registers where each Risk Register has multiple Risk Elements consisting of Causes of Risk, Consequences of Risk, Risk Mitigation Response, Risk Manager Assignments, Risk Category, Risk Status, Likelihood, Impact, Key Risk Indicators, Risk Dates (Creation, Edit, and Due Dates), Total Risk Levels ($), Residual Risk Levels ($), Mitigation Cost, Multiple Risk Controls, and so forth, as illustrated in Figure 8.

Informational Inputs

Multiple Risk Registers (e.g., different projects, business units, investment initiatives, plants, facilities, etc.) can be saved and archived as required, where each Risk Register contains multiple Risk Elements (e.g., the individual risks such as fire, fraud, IT downtime, human errors, accidents, and so forth, within each project, business unit, initiative, facility, etc.), shown as rows in the data grid (Figure 8). The typical qualitative informational inputs include the name of the risk, a short name or acronym, causes of the specific risk, consequences of the risk, any risk mitigation responses, action plans to execute, current status (active or inactive), risk manager it is assigned to, and the Likelihood and Impact levels of the current Risk Element. Risk Category is also a required input and based on the Risk Mapping performed, selecting a specific Risk Category will automatically insert the inputted risk into all mapped relationships, as will be used later in the Risk Dashboards.

Impact and Likelihood

As mentioned, the Risk Register entries require a two-dimensional input of Likelihood (L) or frequency of a risk event occurring and Impact (I) or the severity in terms of financial, economic, and noneconomic effects of the risk. These L and I concepts are industry standard and used even in regulatory environments such as the Basel II and Basel III Accords (initiated by the Bank of International Settlements in Switzerland and accepted by most Central Banks around the world as regulatory reporting standards for operational risks). Alternate measures such as Vulnerability (V), Velocity (υ), and others can be used as well. The whitepaper on applying PEAT ERM at Eletrobrás in Brazil showcases one example of how velocity measures are used.

The uncertainties of repetitive events observed in enterprises' operations over long periods of time can become predictable but usually not with absolute certainty. Such observances can be associated with mathematical functions that reflect the statistical properties of something likely to occur at a future time. The risk of an event occurring is connected to two parameters: the Impact (I) caused by an uncertain event and the probability, or Likelihood (L), of an event occurring. Given some known probability of a risk event occurring, the higher the impact, the greater the risk. If the impact is zero, the risk will be zero even though the event has a high probability of occurring. The reverse argument is also true. If the probability of a risk event occurring is equal to zero, the risk is zero (this is an environment of pure certainty), regardless of the magnitude of the impact.

Risk Mitigation and Total versus Residual Risk

Risk Mitigation, Total Risk, and Residual Risk are the optional monetary inputs in each Risk Element in the Risk Register. Total Risk means the total amount of risk impact this specific Risk Element may cost the organization. The inputs are the projected minimum impact, most likely impact, and maximum impact it might cause. For instance, the risks of a counterparty violating an existing contract may have financial impacts, where the minimal impact might be, say, $0 if the contract is still in force through the end of its term, to a most likely impact of $100,000 in anticipated delays and cost overruns by the counterparty, to a maximum of $300,000 if the counterparty becomes insolvent and subsequent lost business opportunities due to nonperformance of the counterparty. The Mitigation Cost is the amount of money used to reduce the risk exposure of the specific Risk Element, for instance, the cost of obtaining a secondary subcontractor with prenegotiated terms whose contract becomes live only if the original contractor is not performing. Such risk mitigation methods tend to have a financial cost, and the Residual Risk Level as seen in Figure 8 reflects the remaining risk exposure after these risk mitigation strategies have been employed. That is, by having a secondary contract, the risk exposure is a lot less but may still remain.

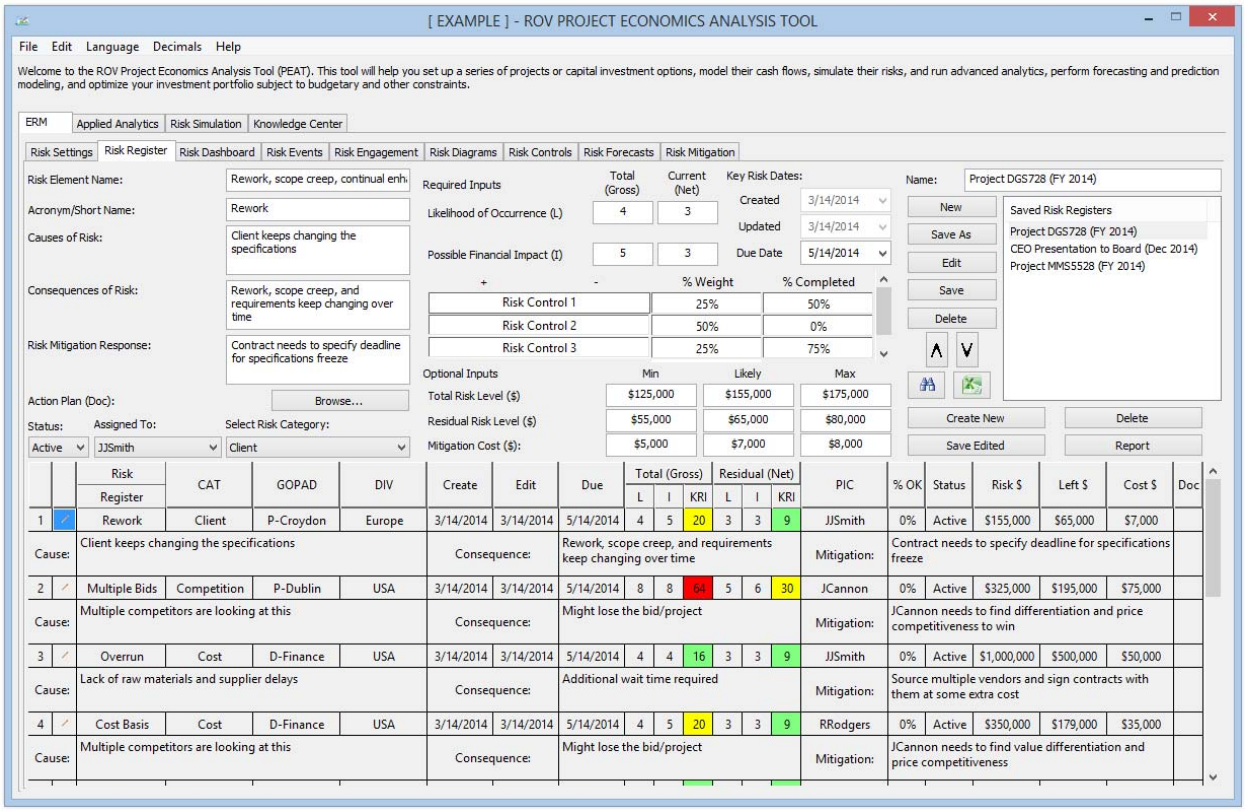


FIGURE 8 Risk Register.

- **Risk Dashboard**

Users of the PEAT ERM system can create multiple types of customized Risk Dashboard views complete with reports, data grids, charts, and visuals, where analysts can select from a specific G.O.P.A.D. category, Division, Risk Category, or Risk Dates. Following are some sample Risk Dashboard views.

Risk Dashboard – Risk Elements

Here KRIs can be viewed using Pareto charts, that is, visual charts on KRI scores across different selected segments, division, or G.O.P.A.D. category of the organization over a specified time span, as shown in Figure 9.

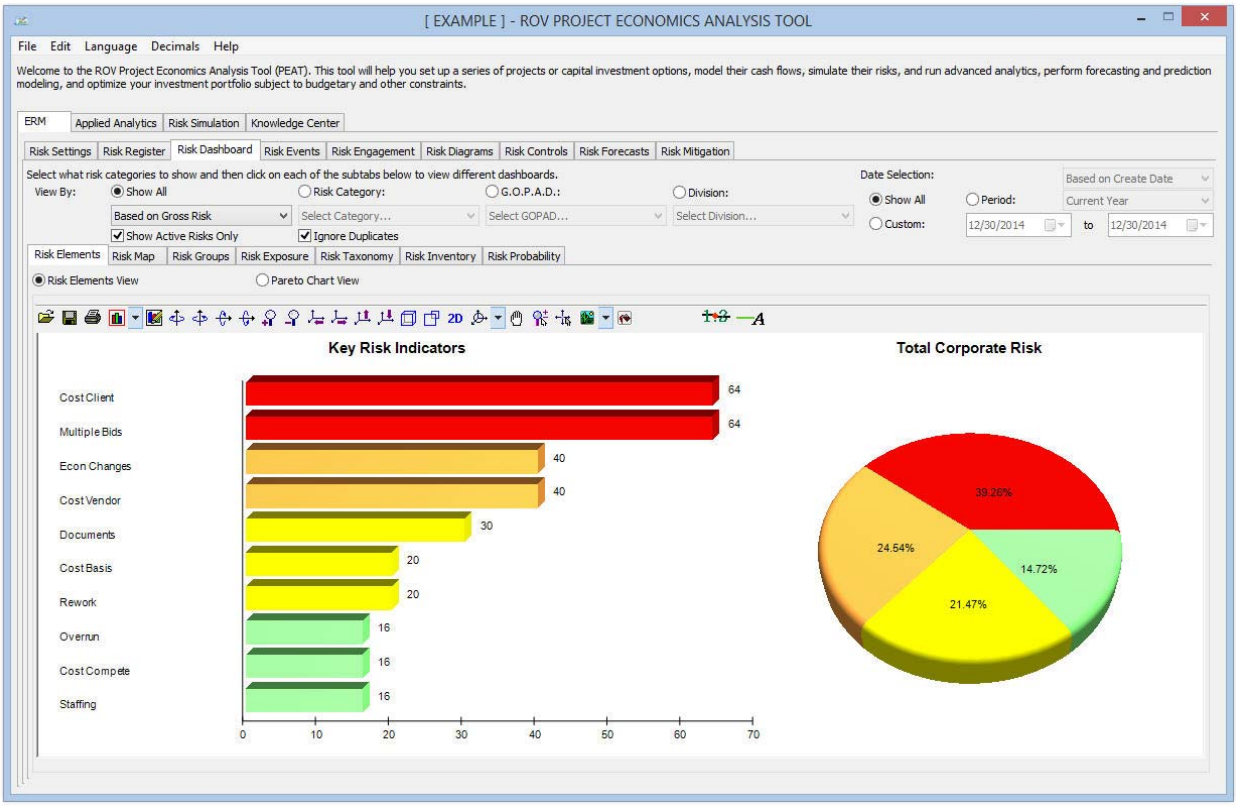


FIGURE 9 Risk Dashboard's risk elements.

Risk Dashboard – Risk Heat Maps

Risk Heat Maps of KRI counts with relevant customizable risk-based color codes across various risk categories, divisions, and segments over specified time periods can also be generated (Figure 10). Each value in the matrix's cells represents the total number of Risk Elements falling within that specific cross section of Likelihood and Impact levels.

Risk Dashboard – Risk Groups

Risk accumulation by G.O.P.A.D. category or other risk groups can be shown as bar charts indicating the Risk Element counts within these selected groups (Figure 11). The ability to slice and dice the data to generate customized reports comes from the previously setup various G.O.P.A.D. components and their mapped relationships to risk types and risk categories.

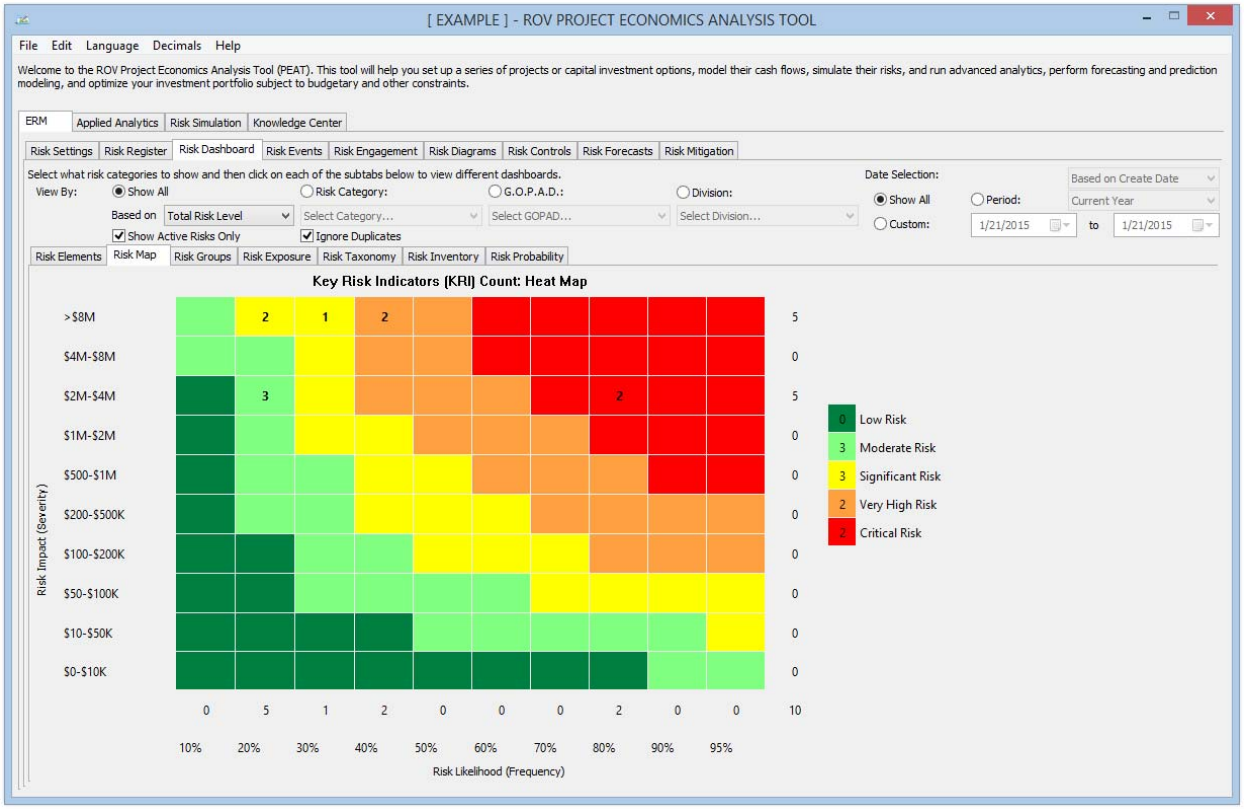


FIGURE 10 Risk Dashboard's risk heat map.

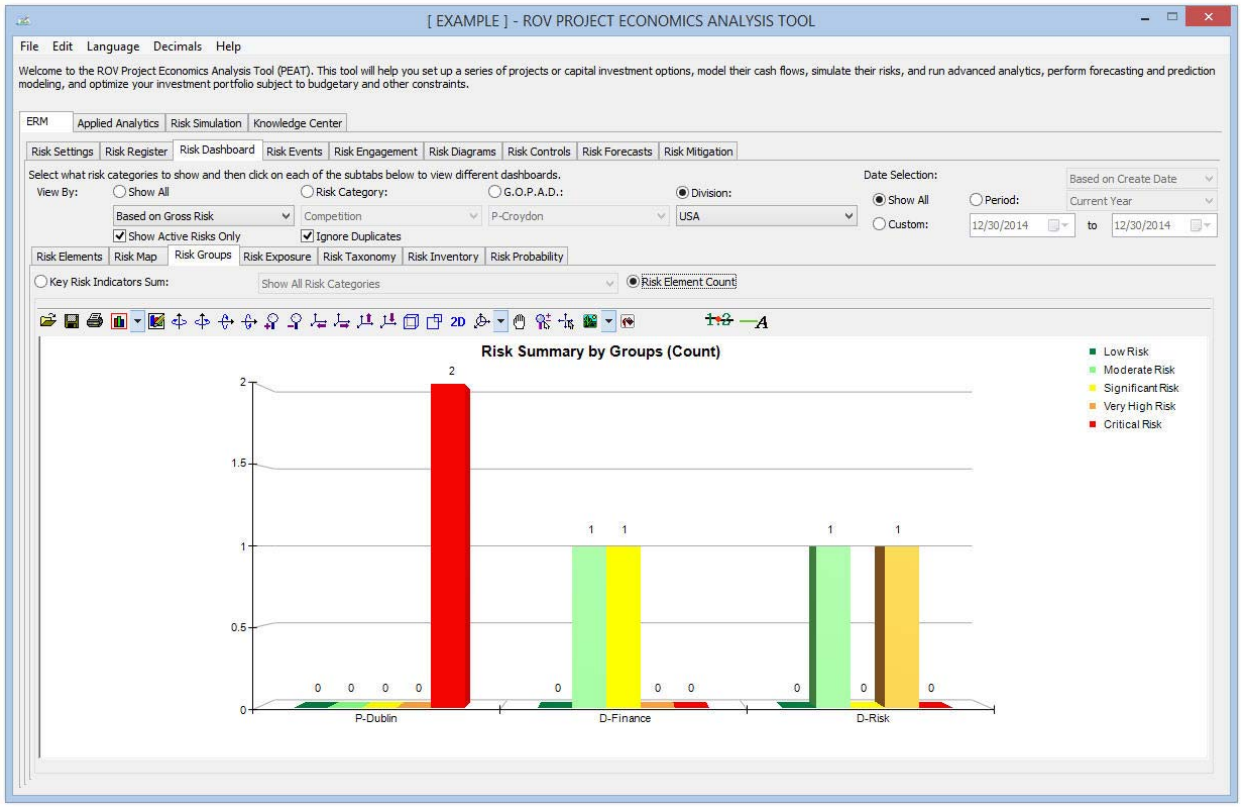


FIGURE 11 Risk Dashboard's Risk Groups (element count by division).

Risk Dashboard – Risk Exposure

The Risk Exposure of a selected segment is shown as risk dials and charts and is compared against the entire Company (Figure 12). These dials and charts represent the Total Risk Exposure and Total Residual Risk Exposure for the selected category and time period, by summing all the relevant Risk Elements' dollar or monetary exposures in the active Risk Register. The default terms of Total Gross Risk (also known as Inherent Risk or Total Risk) and Residual Risk (also known as Active Risk, Remaining Risk, or Current Risk), can all be user-defined in the Risk Settings tab.

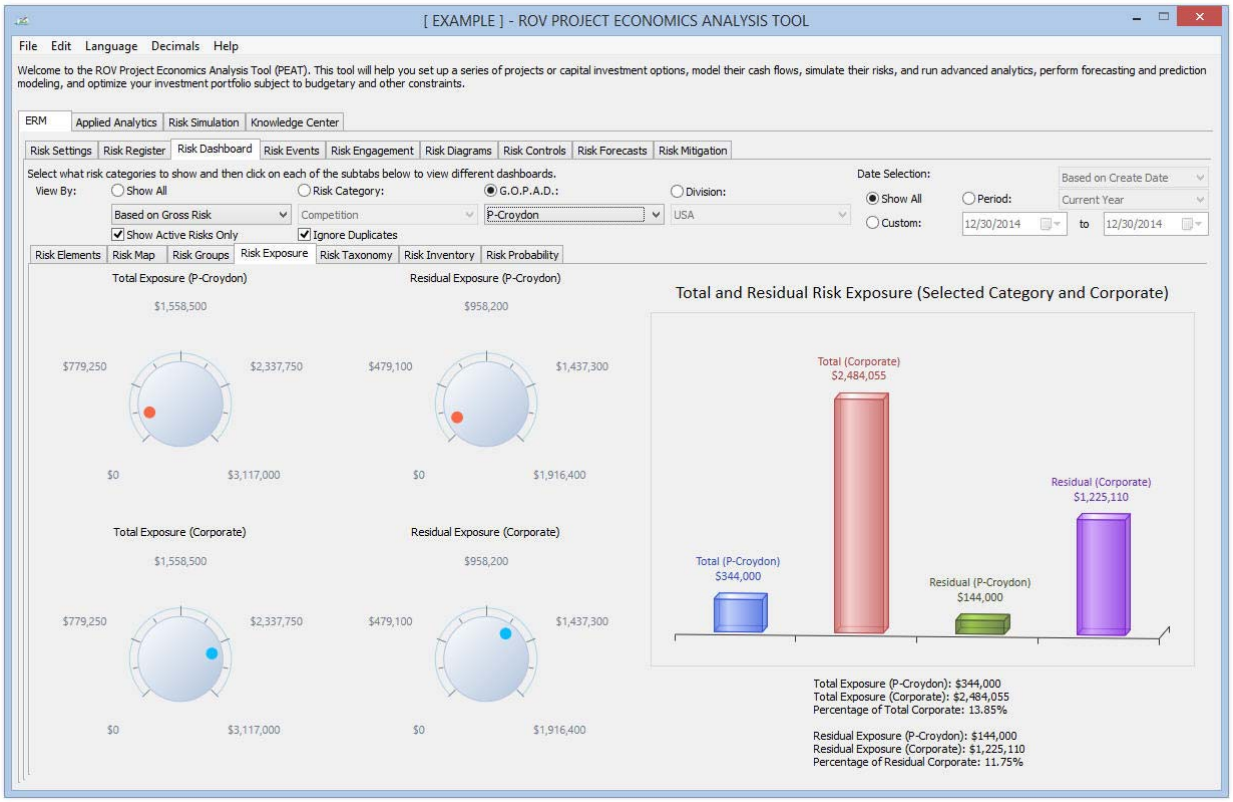


FIGURE 12 Risk Dashboard's Risk Exposure levels (by GOPAD and Corporate).

Risk Dashboard – Risk Taxonomy

This report provides top-down (drill-down) visual representation of the structure of the corporation and its risk associations or Risk Taxonomy, as well as a bottom-up view of how a specific risk permeates throughout the corporation (Figure 13).

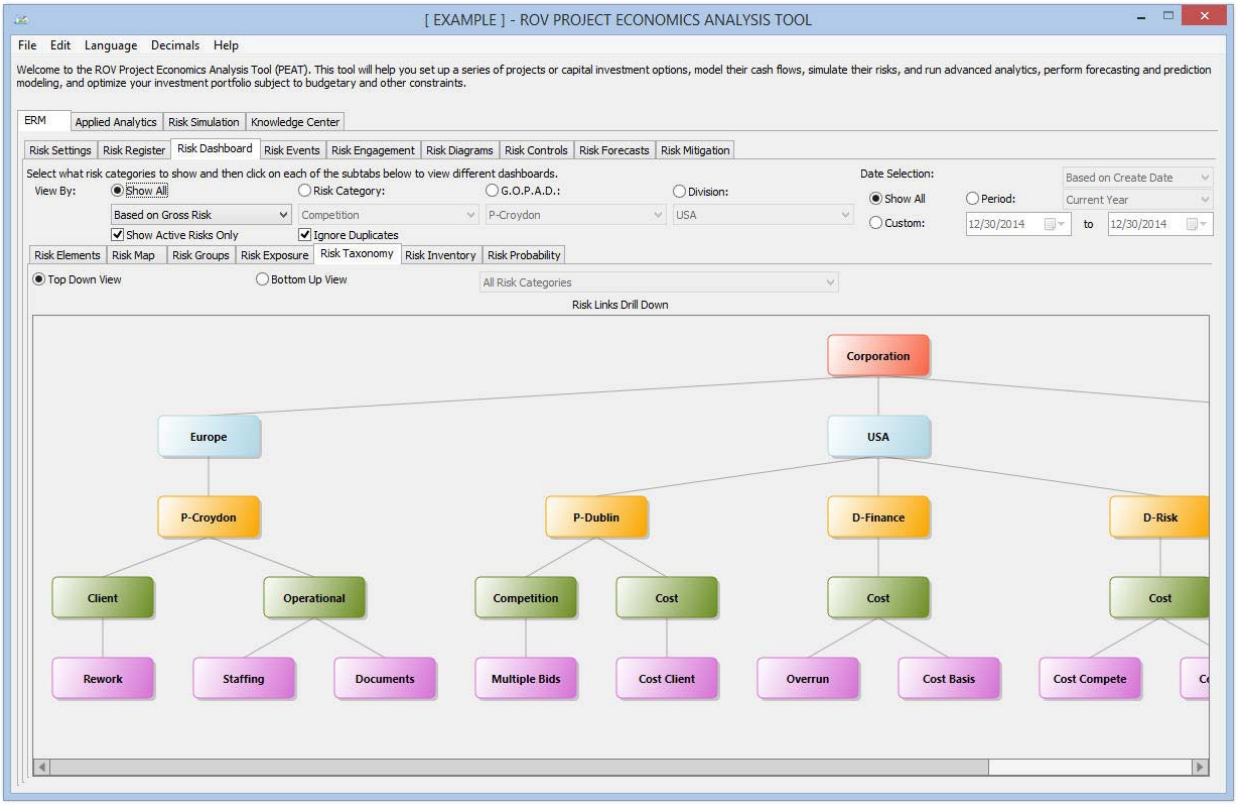
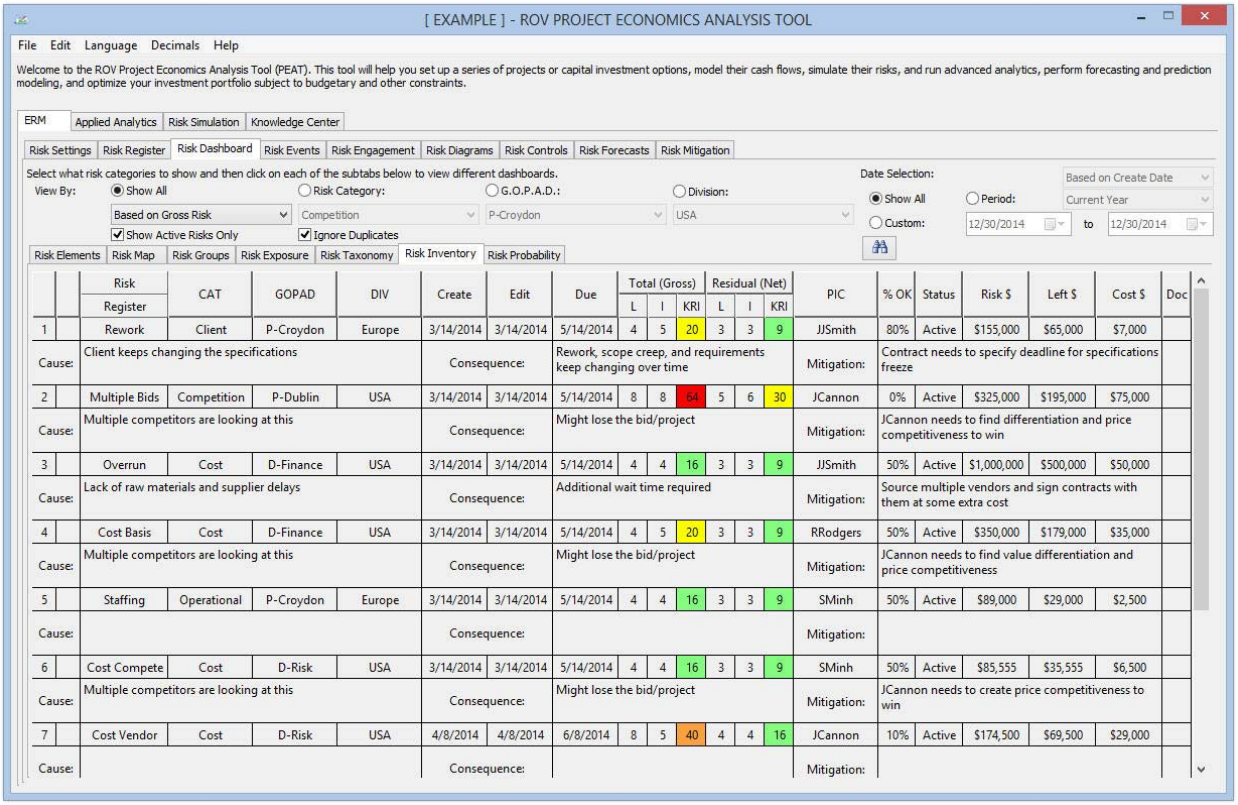


FIGURE 13 Risk Dashboard's Risk Taxonomy (top down view).

Risk Dashboard – Risk Inventory

SQL queries are used to obtain the customized risk profiles and risk reports by Division, G.O.P.A.D. category, Risk Category, Risk Dates, and so forth. The queries will search the active Risk Register for all the relevant Risk Elements that fall within the search parameters and return an inventory of all the risks identified (Figure 14). This report allows for the Risk Monitoring of project management, tasks, completion, and assignments, and it also provides for Risk Governance; provides a Risk Effectiveness Summary, Risk Audit Trail, and Compliance; and complies with International Standards Organization (ISO) Standards. See the whitepaper on how PEAT and ROV technology is in compliance with multiple global risk standards such as COSO, BASEL III, NIST, ISO 31000:2009, and others.



		Risk Register	CAT	GOPAD	DIV	Create	Edit	Due	Total (Gross) L	Total (Gross) I	Total (Gross) KRI	Residual (Net) L	Residual (Net) I	Residual (Net) KRI	PIC	% OK	Status	Risk $	Left $	Cost $	Doc
1		Rework	Client	P-Croydon	Europe	3/14/2014	3/14/2014	5/14/2014	4	5	20	3	3	9	JJSmith	80%	Active	$155,000	$65,000	$7,000	
Cause:		Client keeps changing the specifications				Consequence:		Rework, scope creep, and requirements keep changing over time							Mitigation:	Contract needs to specify deadline for specifications freeze					
2		Multiple Bids	Competition	P-Dublin	USA	3/14/2014	3/14/2014	5/14/2014	8	8	64	5	6	30	JCannon	0%	Active	$325,000	$195,000	$75,000	
Cause:		Multiple competitors are looking at this				Consequence:		Might lose the bid/project							Mitigation:	JCannon needs to find differentiation and price competitiveness to win					
3		Overrun	Cost	D-Finance	USA	3/14/2014	3/14/2014	5/14/2014	4	4	16	3	3	9	JJSmith	50%	Active	$1,000,000	$500,000	$50,000	
Cause:		Lack of raw materials and supplier delays				Consequence:		Additional wait time required							Mitigation:	Source multiple vendors and sign contracts with them at some extra cost					
4		Cost Basis	Cost	D-Finance	USA	3/14/2014	3/14/2014	5/14/2014	4	5	20	3	3	9	RRodgers	50%	Active	$350,000	$179,000	$35,000	
Cause:		Multiple competitors are looking at this				Consequence:		Might lose the bid/project							Mitigation:	JCannon needs to find value differentiation and price competitiveness					
5		Staffing	Operational	P-Croydon	Europe	3/14/2014	3/14/2014	5/14/2014	4	4	16	3	3	9	SMinh	50%	Active	$89,000	$29,000	$2,500	
Cause:						Consequence:									Mitigation:						
6		Cost Compete	Cost	D-Risk	USA	3/14/2014	3/14/2014	5/14/2014	4	4	16	3	3	9	SMinh	50%	Active	$85,555	$35,555	$6,500	
Cause:		Multiple competitors are looking at this				Consequence:		Might lose the bid/project							Mitigation:	JCannon needs to create price competitiveness to win					
7		Cost Vendor	Cost	D-Risk	USA	4/8/2014	4/8/2014	6/8/2014	8	5	40	4	4	16	JCannon	10%	Active	$174,500	$69,500	$29,000	
Cause:						Consequence:									Mitigation:						

FIGURE 14 Risk Dashboard's Risk Inventory.

Risk Dashboard – Risk Probability

This dashboard provides users the ability to compute the PDF/CDF probability of a discrete risk event occurring or continuous risk amounts using historical experience. The analysis is similar to that in Risk Simulator's Distributional Analysis tool, where after a probability distribution is selected and its required input parameters are entered, the PDF and CDF values are returned as a probability table. Figure 15 shows an example situation where a discrete Poisson distribution is selected and the Lambda (mean) value entered is 1.5 (e.g., data was collected for 3 months on the number of errors in bank check deposits per work week at a specific branch of a national bank, and the data shows that there is, on average, 1.5 errors per work week). By setting some starting and ending range and step size, the computed table shows the PDF probability and CDF cumulative probability of a specific risk category's number of events per work week (check deposit errors). The probability that within any work week there will be no check deposit errors is 22.31%, exactly one error is 33.47%, exactly two errors is 25.10%, and so forth. Cumulatively, we can also state that we are 93.44% sure that within any work week, there will be three or fewer risk event errors of the same risk category, assuming history is the best indicator of future performance.

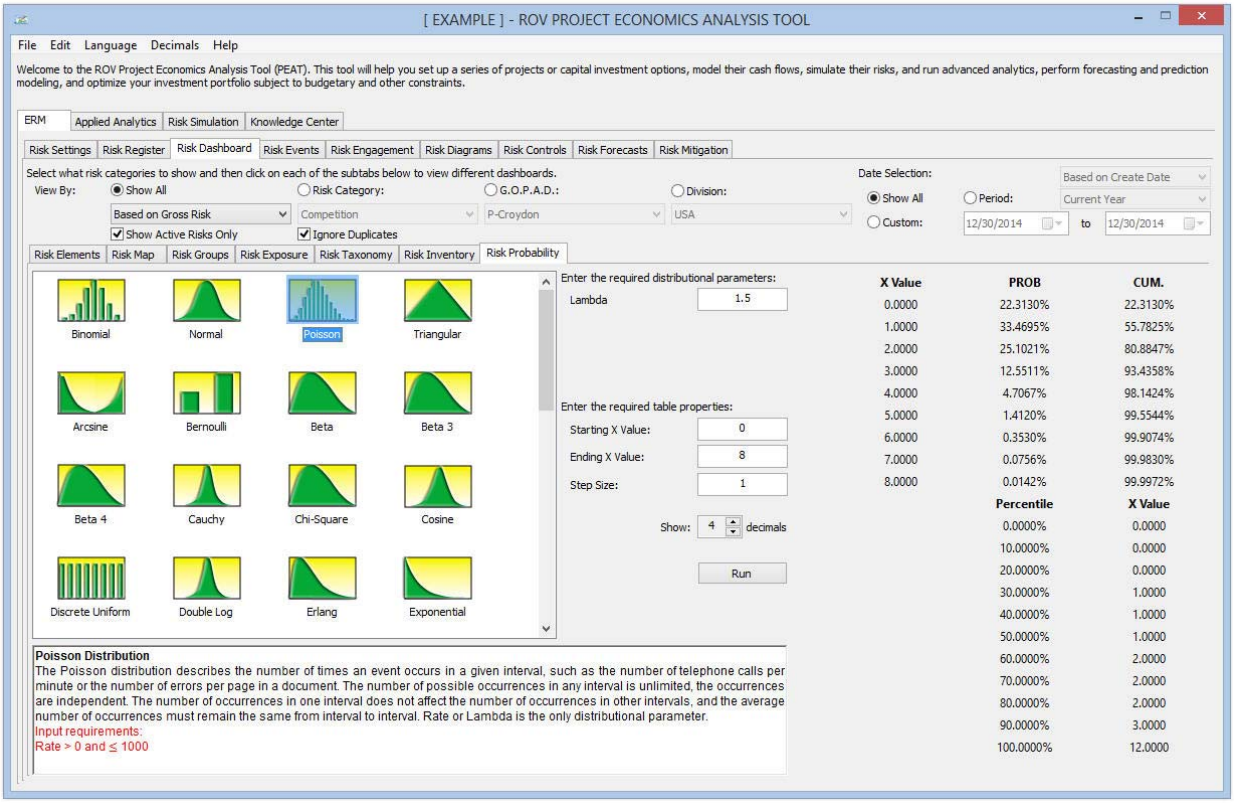


FIGURE 15 Risk Dashboard's exact probability analysis (CDF and PDF).

- **Risk Diagrams**

Users can create Risk Diagrams with ready-made templates on Bowtie Hazard Diagrams, Cause and Effect Ishikawa Fishbone Diagrams, Drill-Down Diagrams, Influence Diagrams, Mind Maps, and Node Diagrams. Sometimes, customized risk diagrams such as those shown in Figure 16 can be used to better illustrate the risk process, risk mitigation, risk cause and effect, and risk impact of the Risk Register. Right-click on the Risk Diagram tab to add additional diagrams or to delete and rename existing diagrams. In addition, various pre-configured diagram templates are available in the droplist to help users get started in generating their own risk diagrams.

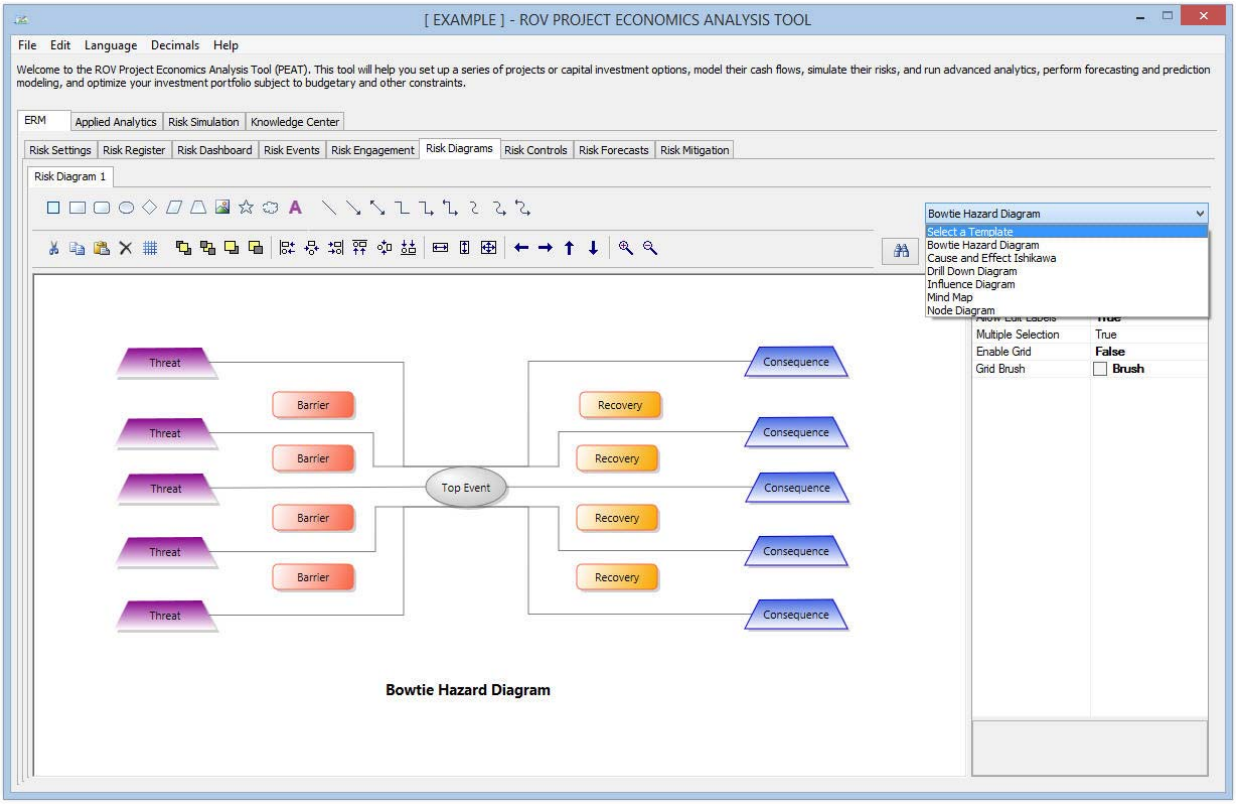


FIGURE 16 Risk Diagrams.

- **Risk Controls**

The PEAT ERM system also allows for the creation of Control Charts and KRI Risk Trends over time (Figure 17), and statistical process controls can be applied to determine if a certain risk element is in- or out-of-control. Control charts help to visually and statistically determine if a specific risk event is in-control or out-of-control. For instance, if the number of risk events such as a plant accident spikes within a certain time period, was that set of events considered expected under statistically normal circumstances or was it an outlier requiring more detailed analysis?

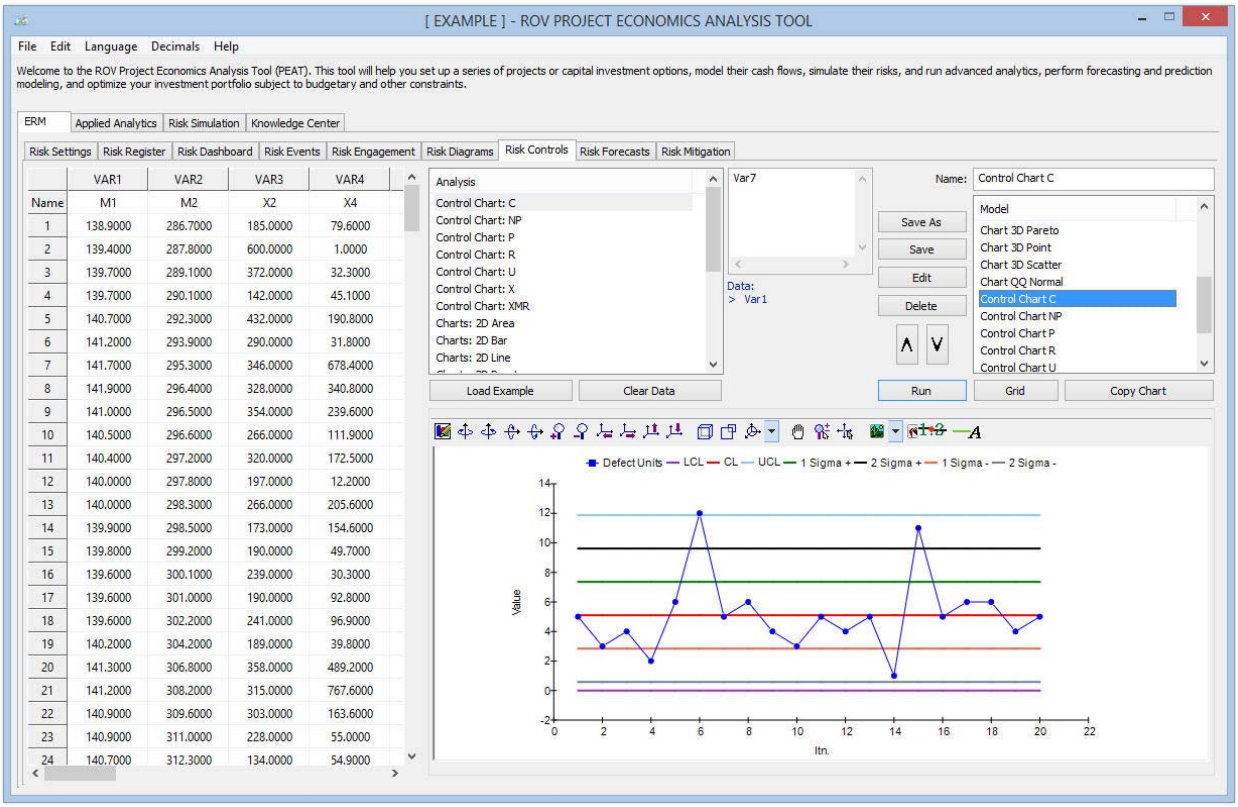


FIGURE 17 Risk Controls charts (sample c-chart).

- **Risk Forecast**

As part of the IRM process, historical risk data can be used to apply predictive modeling to forecast future states of risk, as well as Risk Tracking, Time-Series Risk Forecasts, PDF/CDF Likelihood of Occurrence, and Snapshots per period and over time (Figure 18). Using historical data or subject matter estimates, you can run forecast models on time-series or cross-sectional data by applying advanced forecast analytics such as ARIMA, Auto ARIMA, Auto Econometrics, Basic Econometrics, Cubic Splines, Fuzzy Logic, GARCH (8 variations), Exponential J Curves, Logistic S Curves, Markov Chains, Generalized Linear Models (Logit, Probit, and Tobit), Multivariate Regressions (Linear and Nonlinear), Neural Network, Stochastic Processes (Brownian Motion, Mean-Reversion, Jump-Diffusion), Time-Series Analysis, and Trendlines.

- **Risk Knowledge**

Any good ERM system should always include quick getting started guides and training videos. The Knowledge Center in PEAT's ERM module has slides, training materials, and videos that are all fully customizable for an organization (Figure 19).

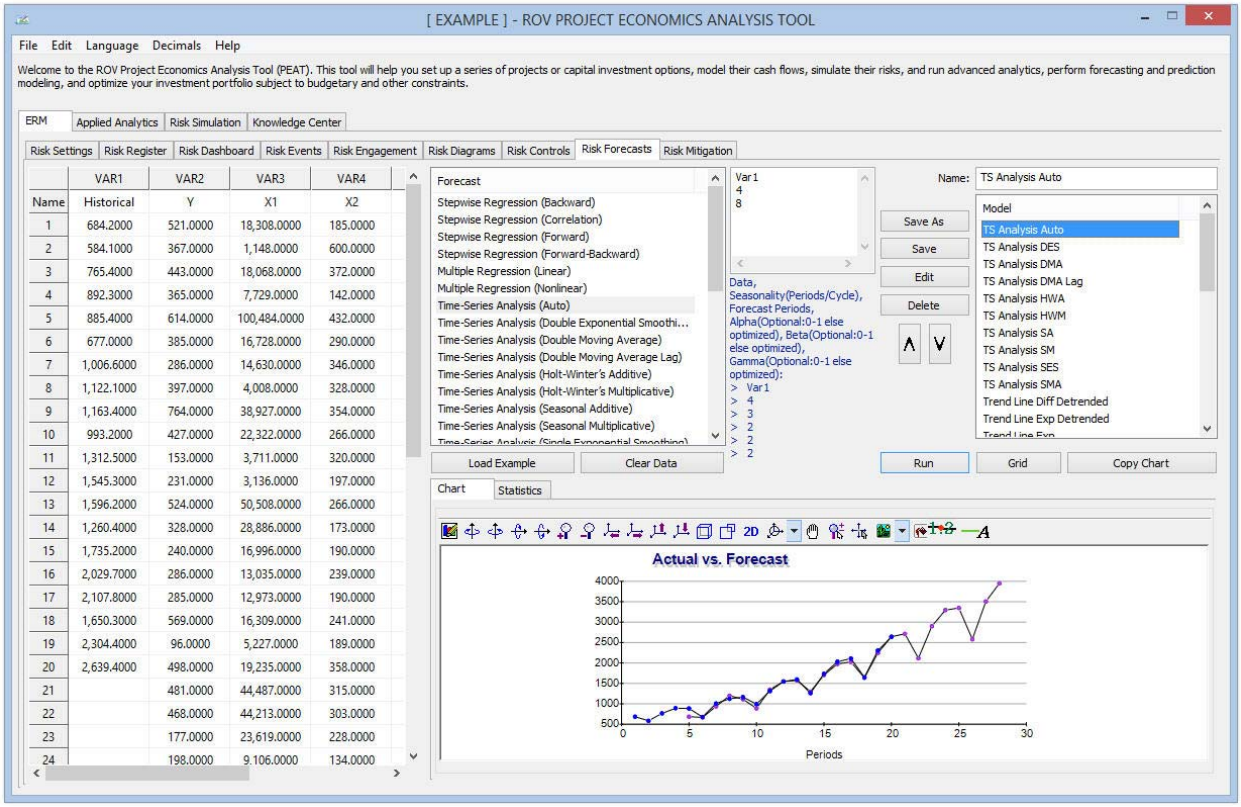


FIGURE 18 Risk forecast.

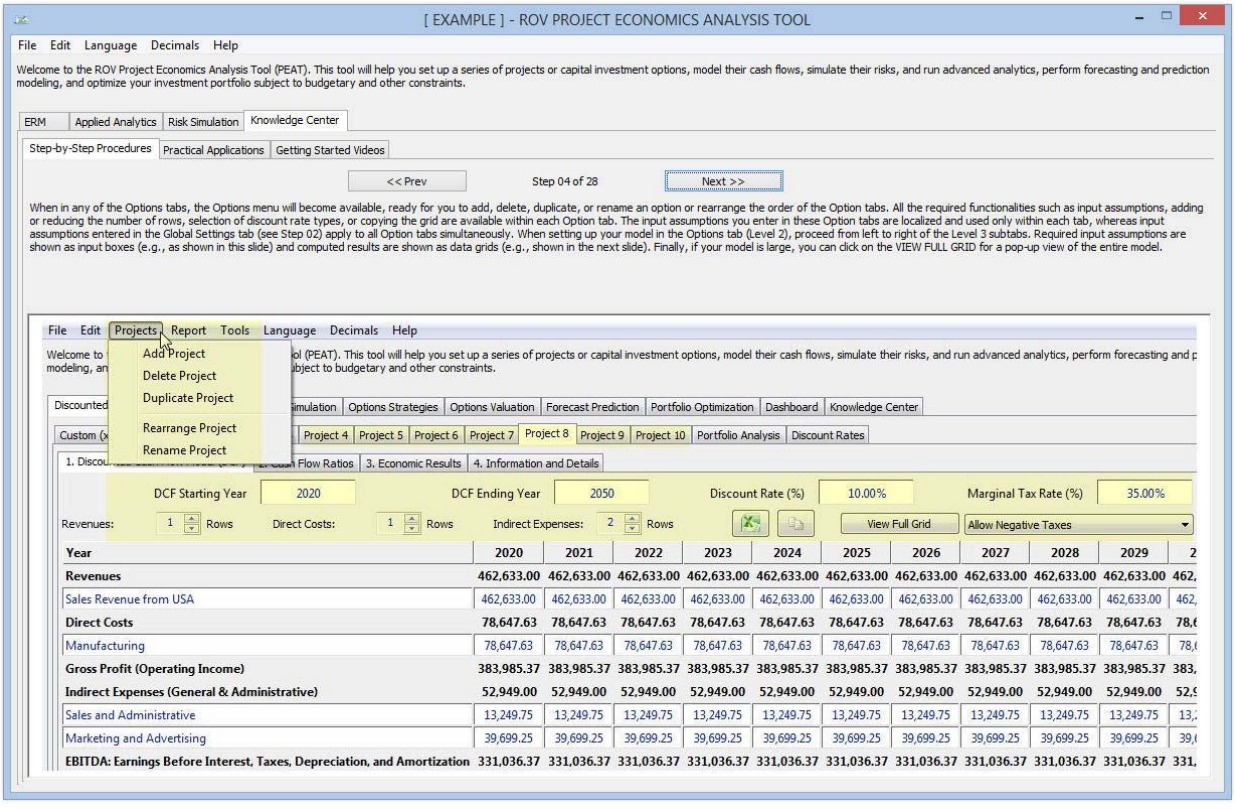


FIGURE 19 Risk Knowledge Center.

- **Risk Mitigation**

The Risk Mitigation analysis in PEAT's ERM helps determine if a specific risk mitigation strategy or technique is working, at least statistically speaking. Risk managers can collect data from *before* and *after* a risk mitigation strategy is implemented and determine if there is a statistically significant difference between the two. The utility allows for the valuation and statistical computation of the effectiveness of risk mitigation programs through various hypothesis testing methods. For example, in the risk event of check deposit errors, the bank could potentially invest in high resolution check scanners with smart optical character recognition software with embedded algorithms to check for any potential human errors. If the number of check errors is tracked before the new scanner system was implemented and compared with after the implementation, risk analysts can determine the efficacy and effectiveness of said scanner, if it was worth the money invested, and if additional scanners should be implemented across other bank branches.

Archiving Risk Events and Risk Engagements

Sometimes Risk Registers can be simplified to not require any Likelihood, Impact, Risk Exposure amounts, Mitigation Costs, or Residual Risk Exposure amounts. That is, only qualitative information and details are required by the organization. Figure 20 shows an illustration of a simplified Risk Register of items in the PEAT ERM system. The risk maps can still be used but only simple risk event counts, event names, and dates are used and captured.

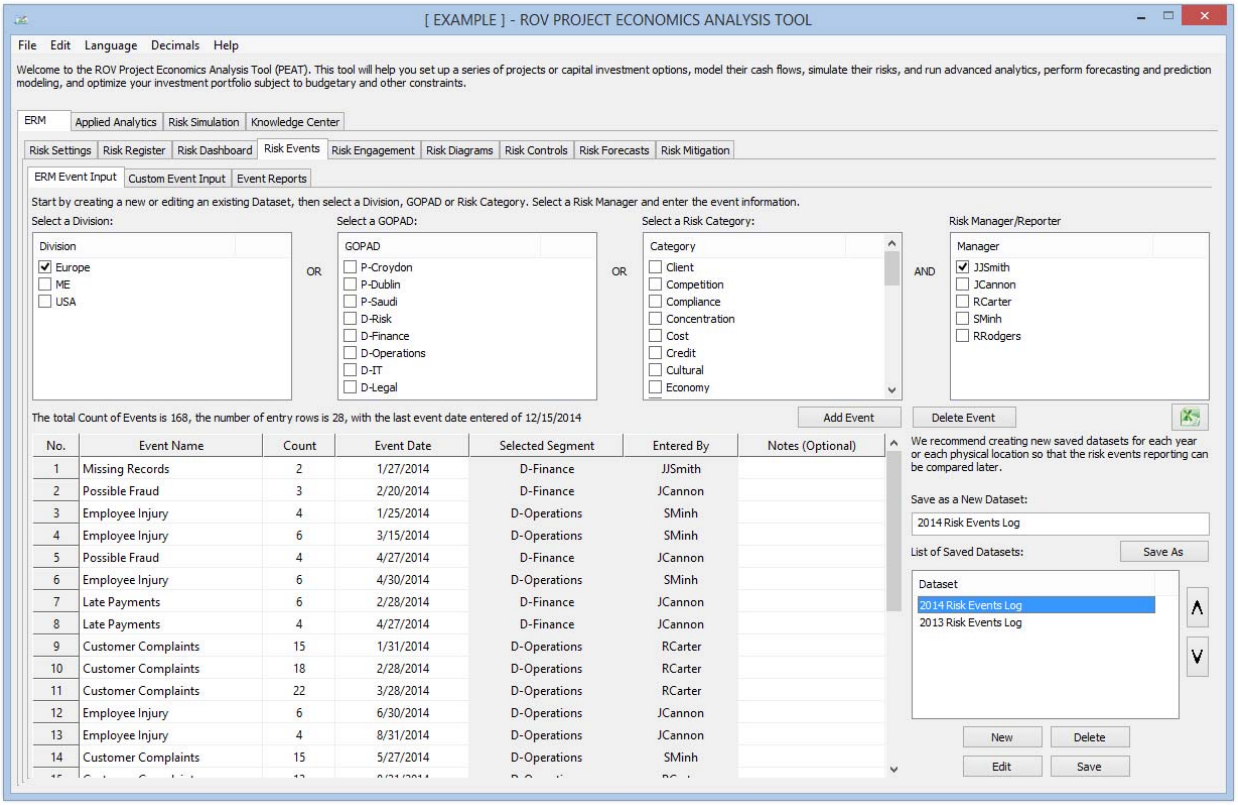


FIGURE 20 Risk Events data entry and archive.

Sometimes, qualitative risk event information needs to be saved and archived. This is where the PEAT ERM's Risk Engagement sections come in handy. Multiple Risk Engagements can be created in a single file where each of the following subsections has multiple Risk Elements: Pre-Engagement Risks, Engagement Risks, and Lessons Learned (Post-Engagement) as seen in Figure 21. By archiving these qualitative risk aspects, a Risk Library can be generated and historical risks can be analyzed over time.

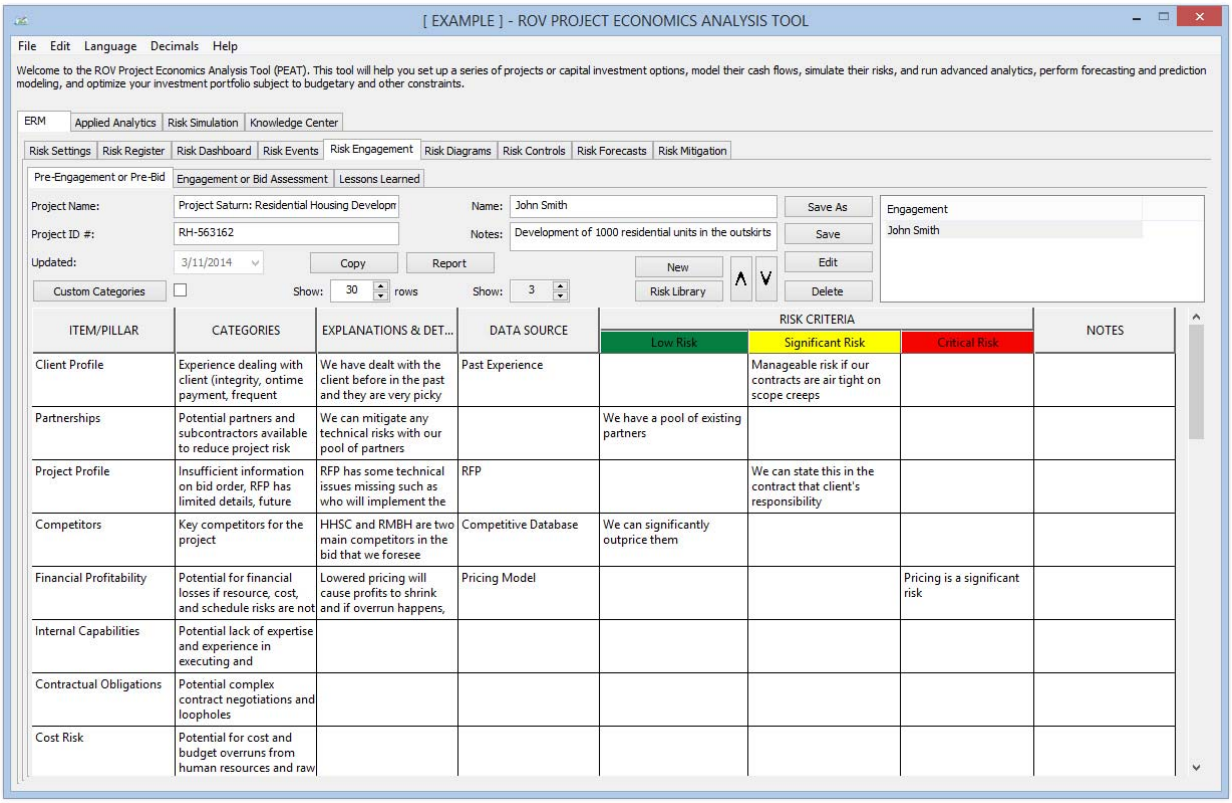


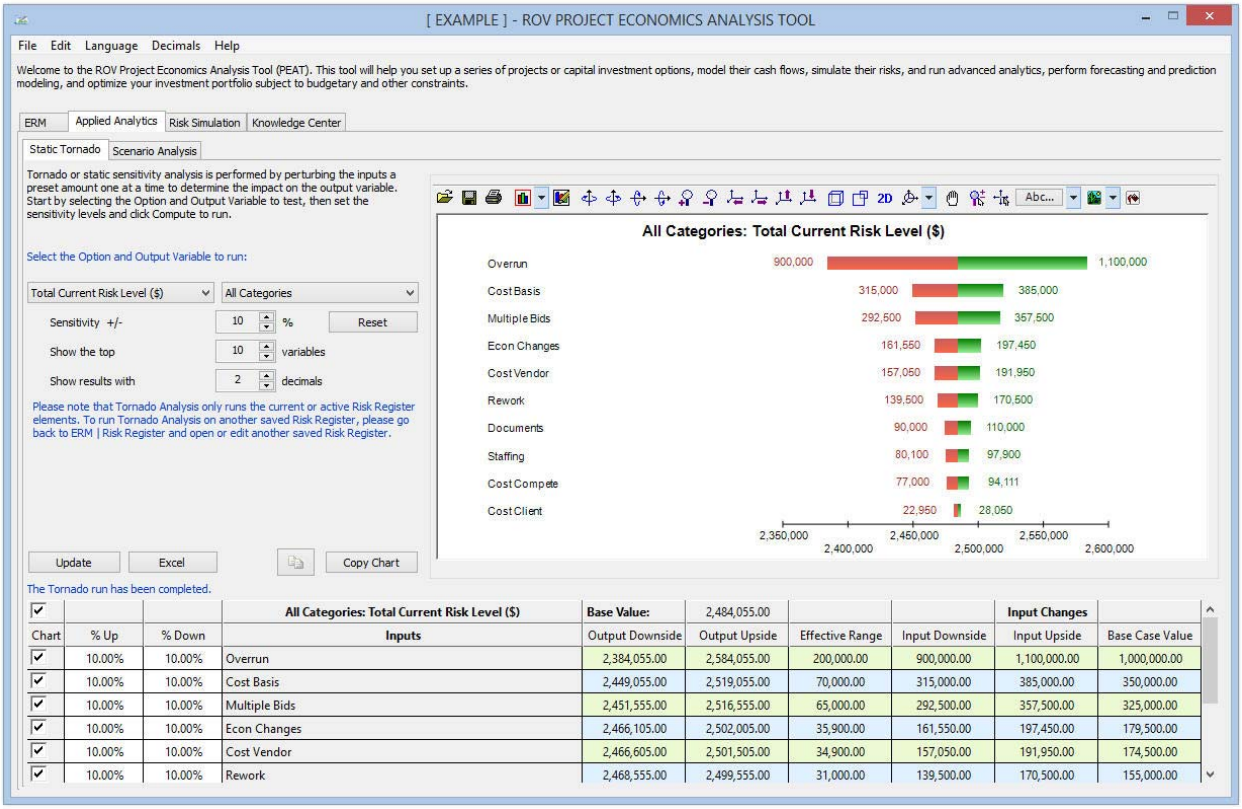
FIGURE 21 Risk Engagement: Pre-Engagement, Engagement, and Lessons Learned.

Bridging the Gap between Qualitative and Quantitative Risk Management

ERM historically has been a qualitative risk management technique. However, in this whitepaper, IRM methods have been applied and interjected into this traditional ERM process. For instance, Likelihood and Impact measures, Total Risk Levels, Residual Risk Levels, and Mitigation Costs are all numerical values. These variables are applicable to each Risk Element in the Risk Register and are Risk Mapped throughout various Risk Segments in the organization. By doing this, we are now able to apply quantitative IRM risk analytics to these values such as Tornado analysis, Monte Carlo Risk Simulations, scenario analysis, heat maps, and other analytics.

ERM Tornado Analysis

As discussed in earlier whitepapers, Tornado analysis helps identify the critical success factors or which risk element contributes the most to the bottom-line risk profile of the company (or risk segment) by statically perturbing each of the risk element's financial risk levels (Figure 22). The same interpretation as discussed in previous whitepapers holds true for Tornado analysis.



			All Categories: Total Current Risk Level ($)	Base Value:	2,484,055.00			Input Changes	
Chart	% Up	% Down	Inputs	Output Downside	Output Upside	Effective Range	Input Downside	Input Upside	Base Case Value
☑	10.00%	10.00%	Overrun	2,384,055.00	2,584,055.00	200,000.00	900,000.00	1,100,000.00	1,000,000.00
☑	10.00%	10.00%	Cost Basis	2,449,055.00	2,519,055.00	70,000.00	315,000.00	385,000.00	350,000.00
☑	10.00%	10.00%	Multiple Bids	2,451,555.00	2,516,555.00	65,000.00	292,500.00	357,500.00	325,000.00
☑	10.00%	10.00%	Econ Changes	2,466,105.00	2,502,005.00	35,900.00	161,550.00	197,450.00	179,500.00
☑	10.00%	10.00%	Cost Vendor	2,466,605.00	2,501,505.00	34,900.00	157,050.00	191,950.00	174,500.00
☑	10.00%	10.00%	Rework	2,468,555.00	2,499,555.00	31,000.00	139,500.00	170,500.00	155,000.00

FIGURE 22 Tornado analysis on ERM risk register elements.

ERM Scenario Analysis

Scenario Analysis helps create multiple risk scenarios of your current or total risk amounts of individual risk elements to determine the impact on the corporate risk profile and to create scenario heat maps.

ERM Monte Carlo Risk Simulations

The PEAT ERM system also allows for the creation of Risk Simulations of the user's risk register element input assumptions via ranges (e.g., minimum, most likely, maximum, average, standard deviation, location, scale, range, percentiles) and returns probabilistic distributions of the individual risk elements or rolled-up risks by categories (output metrics include risk element count, KRI sum, sum and count of risk register elements within a risk category, total risk dollars, total risk mitigation cost, etc.). These probability distributions are automatically generated based on the user's total and residual risk inputs and can be modified and updated as required in the *Set Input Assumptions* tab (Figure 23). The simulated results can be interpreted as usual (Figure 24).

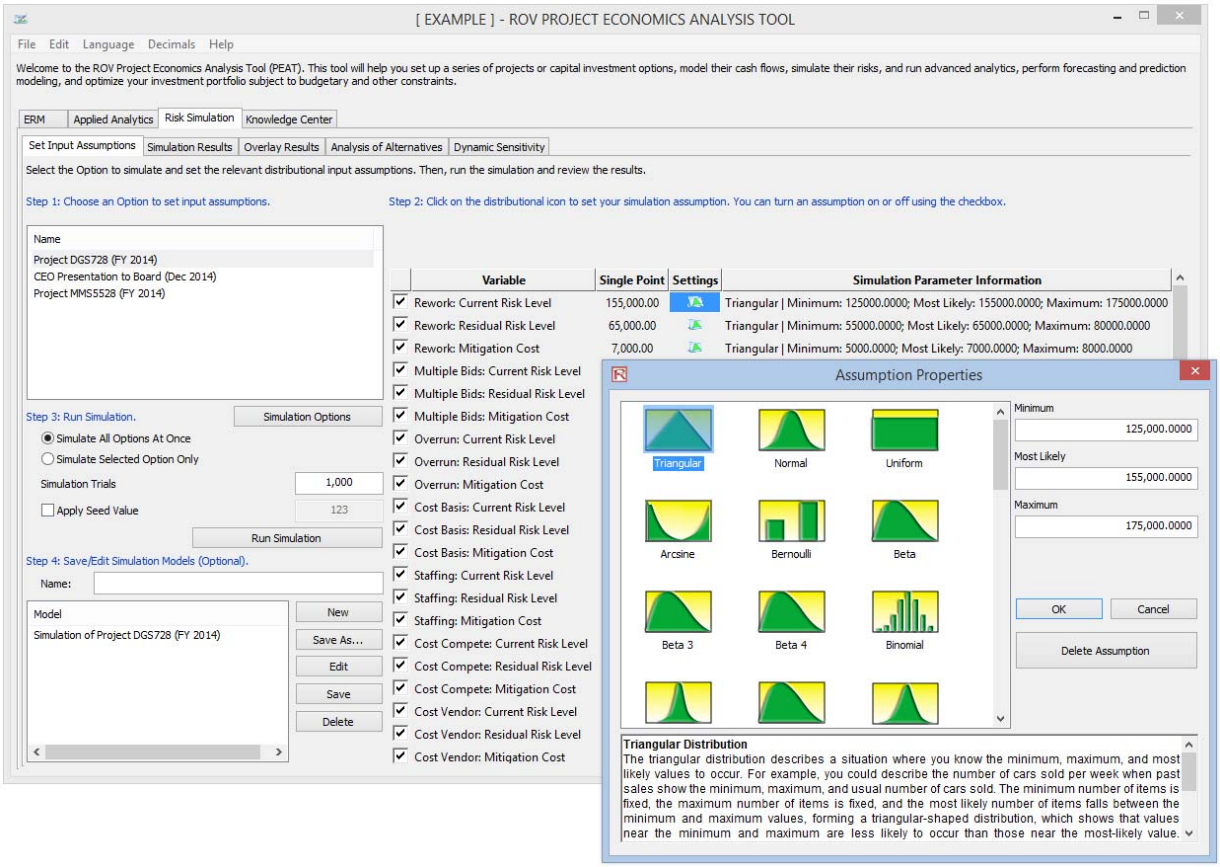


FIGURE 23 Risk Simulation assumptions.

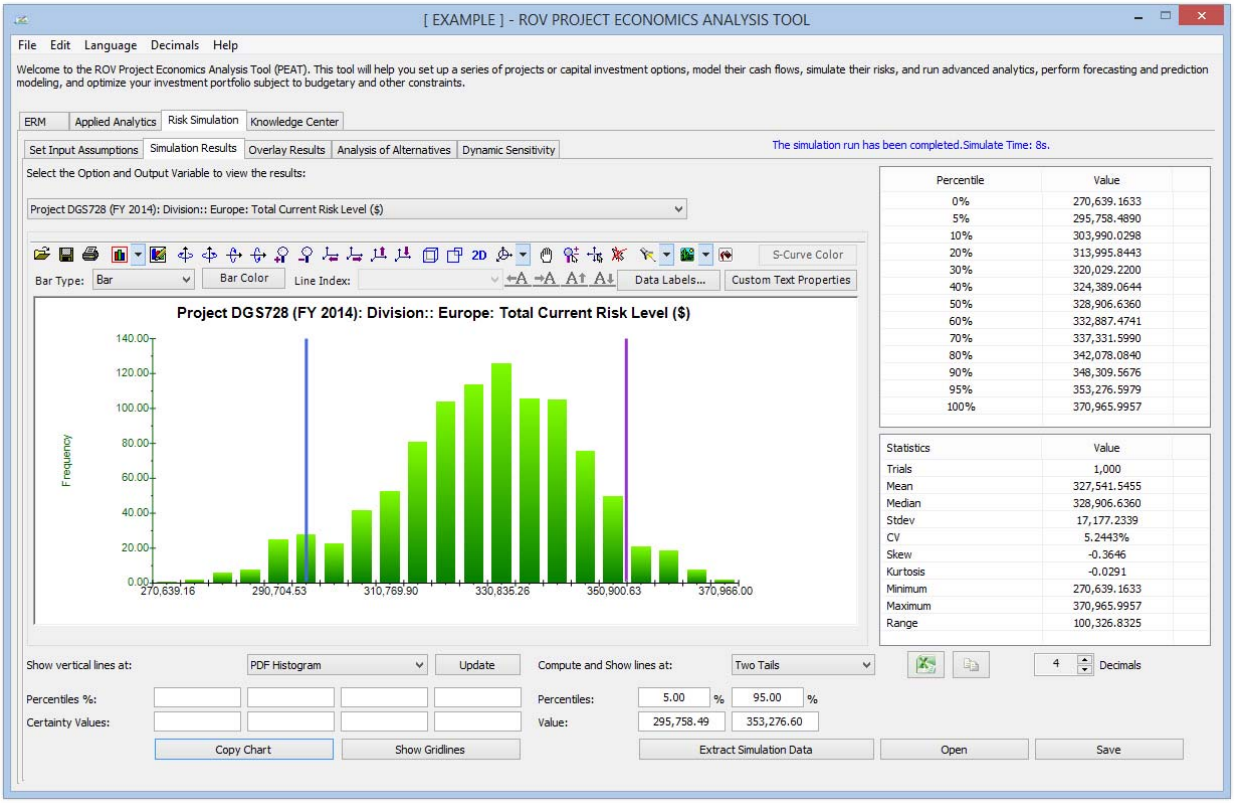


FIGURE 24 Risk Simulation results.

Real Options Valuation, Inc.
4101F Dublin Blvd., Ste. 425, Dublin, California 94568 U.S.A.
www.realoptionsvaluation.com admin@realoptionsvaluation.com

Real Options Valuation Inc