COMPLIANCE WITH GLOBAL STANDARDS: BASEL, COSO, ISO, NIST, & SARBOX

The Enterprise Risk Management (ERM) methods deployed by any organization should at least consider compliance with global standards if not exactly mirroring COSO (Committee of Sponsoring Organizations of the Treadway Commission, with respect to their organizing committees at AAA, AICPA, FEI, IMA, and IIA), International Standards ISO 31000:2009, the U.S. Sarbanes–Oxley Act, the Basel III requirements for Operational Risk (from the Basel Committee through the Bank of International Settlements), and NIST 800-37. The parallels and applications of ROV methodologies closely mirror these regulatory and international standards and, at times, exceed these standards. Figures 1-10 illustrate some examples of compliance with ISO 31000:2009, and Figures 11-20 show compliance with Basel II and Basel III requirements. These figures and the summary lists below assume that the reader is already familiar with the IRM methodology employed by Real Options Valuation, Inc.

**Compliance with International Standards Organization ISO 31000:2009**

The following provides a quick summary pertaining to ISO compliance:

- The IRM methodology we employ is in line with ISO 31000:2009 Clauses 2.3 and 2.8 requiring a risk management process (Figure 1), as well as Clause 5 (5.4.2 requiring risk identification where we use Tornado analysis and scenario analysis; 5.4.3. requiring quantitative risk analysis where we apply Monte Carlo risk simulations; 5.4.4 where existing Excel-based evaluation models are used and overlaid with IRM methodologies such as simulations; etc.). See *Modeling Risk, 3rd Edition*’s Chapter 1 for details on the IRM methodology.

- ISO 31000:2009 Clause 5.4.4 looks at the risk tolerance levels and comparing various risk levels in a portfolio optimization and efficient frontier analysis employed in our IRM methodology (Figure 2). See *Modeling Risk, 3rd Edition*’s Chapters 10 and 11 for optimization and efficient frontier modeling.

- Figure 3 shows quantified consequences and the likelihoods (probabilities and confidence levels) of potential events that can occur using simulations, as required in ISO 31000:2009 Clauses 2.1 and 5.4.3.

- ISO 31000:2009 Clause 5.4.3 requires viewing the analysis from various stakeholders, multiple consequences, and multiple objectives to develop a combined level of risk. This perspective is achieved through a multicriteria optimization and efficient frontier analysis (Figure 4) in the IRM process. See *Modeling Risk, 3rd Edition*’s Chapters 10 and 11 for optimization and efficient frontier modeling.

- ISO 31000:2009 Clause 3F requires that historical data and experience as well as stakeholder feedback and observation coupled with expert judgment be used to forecast future risk events. The IRM process employs a family of 16 forecasting methods (Figure 5 shows an example of the ARIMA model) coupled with risk simulations with high fidelity to determine the best goodness-of-fit when historical data exists, or using subject matter expert estimates and stakeholder assumptions, we can apply the Delphi method and custom distribution to run risk simulations on the forecasts. See *Modeling Risk, 3rd Edition*’s Chapters 8 and 9 for forecast methods and analytical details.
- ISO 31000:2009 Clauses 3C, 5.4.3, 5.5, and 5.5.2 require risk evaluations on risk treatments, options to execute when there are different types of risks, and selecting and implementing various risk treatment strategic options that are not solely reliant on economics. The IRM’s strategic real options methodology allows users to model multiple path-independent and path-dependent implementation strategies or alternate courses of action that are generated to mitigate downside risks and take advantage of upside potentials (Figure 6). See *Modeling Risk, 3rd Edition*’s Chapters 12 and 13 for details on real options analysis modeling techniques.

- Figure 7 illustrates how ISO 31000:2009 Clauses 3D, 3E, and 5.4.3 are satisfied using the IRM process of probability distribution fitting of uncertain variables and how their interdependencies (correlations) are executed.

- Risk controls are required in ISO 31000:2009 Clauses 2.26, 4.43, and 5.4.3 (Figure 8). The control charts and Risk Effectiveness calculations in PEAT ERM help decision makers identify if a particular risk mitigation strategy and response that was enacted had sufficiently and statistically significantly affected the outcomes of future risk states.

- Scenarios, cascading, and cumulative effects (consequences) are also the focus of ISO 31000:2009 Clause 5.4.2. The IRM method employs Tornado analysis, scenario analysis, dynamic sensitivity analysis, and risk simulations (Figure 9) to identify which input(s) have the highest impact on the organization’s risks and model their impacts on the total risks of the organization.

- ISO 31000:2009 Clause 5.2 requires proper communication of risk exposures and consequences, and an understanding of the basis and reasons of each risk. The PEAT ERM Risk Dashboards provide details and insights for a better understanding of the issues governing each of the risk issues in an organization (Figure 10).
FIGURE 1  ISO 31000:2009—IRM.
Investment Efficient Frontiers analysis provides for a variety of budget scenarios when considering portfolios of options.

ISO 31000:2009 (Clause 5.4.4): “Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered. Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risk borne by parties other than the org that benefits from the risk.”

FIGURE 2 ISO 31000:2009—risk tolerance.
Risk Simulation provides the decision maker with additional data

ISO 31000:2009 (Clause 5.4.3): “Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk.”

ISO 31000:2009 (Clause 2.1): “Risk is often characterized by reference to potential events (2.17) and consequences (2.18), or a combination of these.”

FIGURE 3 ISO 31000:2009—consequences and likelihood.
ISO 31000:2009 (Clause 5.4.3): “An event can have multiple consequences and can affect multiple objectives. The way in which consequences and likelihood are expressed and the way in which they are combined determine a level of risk...”

**FIGURE 4** ISO 31000:2009—multiple stakeholder objectives and consequences.
ACTUAL SALES VS. ECONOMETRIC FORECAST
With linkage to the overall economy indicators

ISO 31000:2009 (Clause 3F): “The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecast and expert judgment.”

FIGURE 5
ISO 31000:2009 (Clause 5.4.3): "Risk analysis provides and input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into decision making where choices must be made and the options involve different types and levels of risk."

ISO 31000:2009 (Clause 5.5.3): "Preparing and implementing risk treatment plans..."

ISO 31000:2009 (Clause 5.5.5): "Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls."

ISO 31000:2009 (Clause 5.5.2): "Selection of risk treatment options."

ISO 31000:2009 (Clause 5.5.2): "Decisions should also take into account risks which can be dealt with at lower cost but are not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks."

ISO 31000:2009 (Clause 3C): "RM is part of decision making. RM helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action."

**FIGURE 6** ISO 31000:2009—multiple options, strategies, and alternatives.
FIGURE 7

ISO 31000:2009 structured approach, fitting, and correlations.
Operational Risk Controls

FIGURE 8  ISO 31000:2009—risk control efficiency and effectiveness.
ISO 31000:2009 (Clause 5.4.2): “Risk Identification: Risk identification should include examination of the knock-on effect of particular consequences, including cascade and cumulative effects. It is necessary to consider possible causes and scenario that show what consequence can occur.”

FIGURE 9 ISO 31000:2009—consequences, cascades, and scenarios.
Management Dashboards

ISO 31000:2009 (Clause 5.2): “Communication and consultation with external and internal stakeholders should take place during all stages of the RM process. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Stakeholders need to understand the basis on which decisions are made, and the reasons why particular actions are required.”

FIGURE 10 ISO 31000:2009—communication and consultation.
Compliance with Basel II and Basel III Regulatory Requirements

The following provides a summary of Basel II and Basel III compliance when using the IRM methodology:

- Figure 11 shows Monte Carlo risk simulations applied to determine confidence levels, percentiles, and probabilities of occurrence using historically fitted data or forecast expectations. These methods are in line with Basel II and Basel III requirements Sections 16 and 161 concerning the use of historical simulations, Monte Carlo simulations, and 99th percentile confidence intervals. See *Modeling Risk, 3rd Edition*'s Chapters 5 and 6 for details on simulations and data fitting techniques.

- Figure 12 shows a correlated simulation of a portfolio of assets and liabilities, where asset returns are correlated against one another in a portfolio and optimization routines were run on the simulated results. These processes provide compliance with Basel II and Basel III requirements Sections 178, 232, and 527(f) involving correlations, Value at Risk or VaR models, portfolios of segments, and pooled exposures (assets and liabilities). See *Modeling Risk, 3rd Edition*'s Chapter 5 for correlated simulations and Chapter 7's case study on Basel II and Basel III Credit, Market, Operational, and Liquidity Risks with Asset Liability Management for details on how VaR models are computed based on historical simulation results.

- Figure 13 shows Value at Risk percentile and confidence calculations using structural models and simulation results that are in line with Basel II and Basel III requirements Sections 179, 527(c), and 527(f). As noted above, see *Modeling Risk, 3rd Edition*'s Chapter 7's case study for details on how VaR models are computed based on historical simulation results.

- Figure 14 shows the computations of probability of default (PD) as required in the Basel Accords, specifically Basel II and Basel III Section 733 and Annex 2's Section 16. PD can be computed using structural models or based on historical data through running basic ratios to more advanced binary logistic models. *Modeling Risk, 3rd Edition*'s Chapter 7's case study as well as Chapter 14's *Credit and Market Risk* case study provide more insights into how PD can be computed using these various methods.

- Figure 15 shows the simulation and generation of interest rate yield curves using Risk Simulator and Modeling Toolkit models. These methods are in line with Basel II and Basel III requirements Section 763 requiring the analysis of interest rate fluctuations and interest rate shocks.

- Figure 16 shows additional models for volatile interest rate, financial markets, and other liquid instruments' instantaneous shocks using Risk Simulator's stochastic process models. These analyses conform to Basel II and Basel III requirements Sections 155, 527(a), and 527(b).

- Figure 17 shows several forecast models with high predictive and analytical power, which is a part of the Risk Simulator family of forecast methods. Such modeling provides compliance with Basel II and Basel III requirements Section 417 requiring models of good predictive power.

- Figure 18 shows the list of financial and credit models available in the ROV Modeling Toolkit and ROV Real Options SLS software applications. These models conform to Basel II and Basel III requirements Sections 112, 203, and 527(e) requiring the ability to value over-the-counter (OTC) derivatives, nonlinear equity derivatives, convertibles, hedges, and embedded options.

- Figure 19 shows the modeling of foreign exchange instruments and hedges to determine the efficacy and effectiveness of foreign exchange hedging vehicles and their impact on valuation, portfolio profitability, and VaR, in line with Basel II and Basel III Sections 131 and 155 requiring the analysis of different currencies, correlations, volatility, and hedges.

- Figure 20 shows the option-adjusted spread (OAS), credit default swaps (CDS), and credit spread options (CSO) models in ROV Modeling Toolkit. These models provide compliance with Basel II and Basel III requirements Sections 140 and 713 pertaining to modeling and valuing credit derivatives and credit hedges.
FIGURE 11  Basel II/III confidence levels, Monte Carlo simulations, and credit risk.
Basel III Compliance

Correlated Portfolio Optimization

FIGURE 12 Basel II/III correlated portfolios and correlated simulations.

Basel II & III Section 178:
As an alternative to the use of standard or own-estimate haircuts, banks may be permitted to use a VaR models approach to reflect the price volatility of the exposure and collateral for repo-style transactions, taking into account correlation effects between security positions. This approach would apply to repo-style transactions covered by bilateral netting agreements on a counterparty-by-counterparty basis.

Basel II & III Section 232
The exposure must be one of a large pool of exposures, which are managed by the bank on a pooled basis. Furthermore, it must not be managed individually in a way comparable to corporate exposures, but rather as part of a portfolio segment or pool of exposures with similar risk characteristics for purposes of risk assessment and quantification.

Basel II & III Section 527 (f):
Subject to supervisory review, equity portfolio correlations can be integrated into a bank’s internal risk measures. The use of explicit correlations (e.g., utilization of a variance/covariance VaR model) must be fully documented and supported using empirical analysis. The appropriateness of implicit correlation assumptions will be evaluated by supervisors in their review of model documentation and estimation techniques.
Basel III Compliance

Value at Risk

FIGURE 13 Basel II/III Value at Risk and percentiles.

Basel II & III Section 179:
The quantitative and qualitative criteria for recognition of internal market risk models for repo-style transactions and other similar transactions are in principle the same as under the Market Risk Amendment. With regard to the holding period, the minimum will be 5-business days for repo-style transactions, rather than the 10-business days under the Market Risk Amendment. For other transactions eligible for the VaR models approach, the 10-business day holding period will be retained.

Basel II & III Section 527 (c):
No particular type of VaR model (e.g., variance-covariance, historical simulation, or Monte Carlo) is prescribed. However, the model used must be able to capture adequately all of the material risks embodied in equity returns, including both the general market risk and specific risk exposure of the Institution's equity portfolio. Internal models must adequately explain historical price variation, capture both the magnitude and changes in the composition of potential concentrations, and be robust to adverse market environments. The population of risk exposures represented in the data used for estimation must be closely matched to or at least comparable with those of the bank's equity exposures.

Basel II & III Section 527 (f):
Subject to supervisory review, equity portfolio correlations can be integrated into a bank's internal risk measures. The use of explicit correlations (e.g., utilization of a variance-covariance VaR model) must be fully documented and supported using empirical analysis. The appropriateness of implicit correlation assumptions will be evaluated by supervisors in their review of model documentation and estimation techniques.
Financial Engineering: Credit Risk

FIGURE 14 Basel II/III credit risk analysis.

Basel II & III Annex 2 - Section 16:
After reviewing a variety of methodologies, the Committee decided to use Monte Carlo simulations to calibrate both the monitoring and trigger levels for each credit risk assessment category. In particular, the proposed monitoring levels were derived from the 99th percentile confidence interval and the trigger level benchmark from the 99.9th percentile confidence interval.

Basel II & III Section 733:
Credit risk: Banks should have methodologies that enable them to assess the credit risk involved in exposures to individual borrowers or counterparties as well as at the portfolio level. For more sophisticated banks, the credit review assessment of capital adequacy, at a minimum, should cover four areas: risk rating systems, portfolio analysis/aggregation, securitization/complex credit derivatives, and large exposures and risk concentrations.
Financial Engineering: Market Risk

Interest Rate and Yield Curve Analytics

**FIGURE 15** Basel II/III interest rate risk and market shocks.

Basel II & III Section 753:
The revised guidance on interest rate risk recognizes banks’ internal systems as the principal tool for the measurement of interest rate risk in the banking book and the supervisory response. To facilitate supervisors’ monitoring of interest rate risk exposures across institutions, banks would have to provide the results of their internal measurement systems, expressed in terms of economic value relative to capital, using a standardized interest rate shock.
Financial Engineering: Market Risk

- ARIMA
- GARCH Volatility
- Brownian Motion Random Walk
- Cubic Spline Yield Curves
- Implied Yield Curves from Debt
- Mean-Reverting Interest Rates
- Jump-Diffusion Prices
- Mixed Stochastic Processes
- Time-Series Decomposition

FIGURE 16

Basel II/III volatility and adverse instantaneous shocks.

Basel II & III Section 527 (a) and (b):
The capital charge is equivalent to the potential loss on the institution’s equity portfolio arising from an assumed instantaneous shock equivalent to the 99th percentile, one-tailed confidence interval of the difference between quarterly returns and an appropriate risk-free rate computed over a long-term sample period. The estimated losses should be robust to adverse market movements relevant to the long-term risk profile of the institution’s specific holdings.

Basel II & III Section 155:
Banks must estimate the volatility of the collateral instrument or foreign exchange mismatch individually. Estimated volatilities for each transaction must not take into account the correlations between unsecured exposure, collateral, and exchange rates.
Data and Relationship Modeling

Econometric Analysis - ARIMA, Regressions, GARCH

Modeling and forecasting cross-sectional, time-series, and panel data, and applications of volatility forecasts.

FIGURE 17 Basel II/III forecast models with strong predictive power.
FIGURE 18    Basel II/III modeling OTC derivatives and exotic convertibles.
FIGURE 19  Basel II/III modeling foreign exchange fluctuations.
Credit Derivatives

FIGURE 20 Basel II/III credit derivatives and hedging.
Compliance with COSO Integrated ERM Framework

The following provides a quick summary of COSO Integrated ERM Framework compliance when using the IRM methodology:

- Figure 21 (16.45) shows the PEAT ERM module's Risk Register tab where mitigation costs and benefits (gross risks reduced to residual risk levels), likelihood and impact measures, and spreads with varying precision levels ready for Monte Carlo risk simulation are situated, in compliance with COSO ERM Framework Sections 5 & 6.
- Figure 22 (16.46) shows the PEAT ERM module where the likelihood and impact within a risk map is generated, in compliance with COSO AT/Exhibit 5.13.
- Figure 23 (16.47) shows compliance with COSO AT/Exhibit 6.5 and COSO ERM Integrated Framework Section 6, where entity-wide portfolio and business unit, department, and functional areas' gross and residual risks are computed.
- Figure 24 (16.48) continues by showing a sample of the Risk Dashboard reports also in compliance with COSO AT/Exhibit 6.5 and COSO ERM Integrated Framework Section 6, where entity-wide portfolio and business unit, department, and functional areas' gross and residual risks are computed and compared against each other.
- Figure 25 (16.49) shows the PEAT DCF module's efficient frontier model, consistent with COSO AT/Exhibit 3.7 requiring an analysis of the capital investment in relation to the returns within a diversified (optimized) portfolio.
- Figure 26 (16.50) shows the PEAT ERM and DCF modules' simulated results, where Value at Risk, percentiles, and statistical probabilities can be obtained, in compliance with COSO AT/Exhibit 5.5 requiring a range of outcomes based on distributional assumptions, and COSO ERM Integrated Framework Exhibit 5.2 requiring historical or simulated outcomes of future behaviors under probabilistic models.
- Figure 27 (16.51) shows compliance with COSO AT/Exhibit 3.1 requiring the use of scenario modeling and stress testing.
- Figure 28 (16.52) shows the CMOL module in PEAT where scenario analysis, stress testing, and gap analysis are performed, in compliance with COSO AT/Exhibit 5.10, to complement probabilistic models.
- Figure 29 (16.53) shows compliance with COSO AT/Exhibits 5.8 & 5.9 requiring the modeling of operational and credit loss distributions with back-testing or historical simulation, sensitivity analysis, and Value at Risk calculations.
FIGURE 21  PEAT ERM and COSO Integrated Framework.
FIGURE 22    PEAT ERM heat map and risk matrix.
FIGURE 23  PEAT ERM portfolio and corporate view or residual risk.

COSO ERM Integrated Framework, Section 8: Portfolio View: Enterprise risk management requires that risk be considered from an entity-wide, or portfolio perspective. Management typically takes an approach in which risk first is considered for each business unit, department, or function, with the responsible manager developing a composite assessment of risks for the unit reflecting the unit’s residual risk profile relative to its objectives and risk tolerances.

COSO Application Techniques, Exhibit 8.5: Portfolio View of Residual Risk: With a view of risk for individual units, an enterprise’s senior management is well positioned to take a portfolio view, to determine whether the entity’s residual risk profile is commensurate with its overall risk appetite relative to its objectives.
COSO ERM Integrated Framework, Section 6: Portfolio View:
Enterprise risk management requires that risk be considered from an entity-wide, or portfolio perspective. Management typically takes an approach in which risk first is considered for each business unit, department, or function, with the responsible manager developing a composite assessment of risks for the unit reflecting the unit's residual risk profile relative to its objectives and risk tolerances.

COSO Application Techniques, Exhibit 5.5: Portfolio View of Residual Risk:
With a view of risk for individual units, an enterprise’s senior management is well positioned to take a portfolio view, to determine whether the entity’s residual risk profile is commensurate with its overall risk appetite relative to its objectives.

FIGURE 24  PEAT ERM portfolio, business unit, department, function view
FIGURE 25  PEAT DCF module featuring capital versus returns efficient frontier
FIGURE 26  PEAT ERM & DCF modules with risk simulation results with Value at Risk
COSO Application Technique, Exhibit 3.1: Scenarios, Stress Testing, Modeling
Using scenario analysis, modeling, and stress testing, management compared the results of each option in relation to the impact on return on capital employed. Management identified the distribution of potential return outcomes.

**FIGURE 27** PEAT ERM & DCF modules with scenario analysis and heat map regions
COSO Application Techniques, Exhibit 5.10: Scenario Testing and Stress Testing

Scenario analysis assesses the effect on an objective of one or more events. Stress testing assesses the impact of events having extreme impact. Stress testing differs from scenario analysis in that it focuses on the direct impact of a change in only one event or activity under extreme circumstances, as opposed to focusing on changes on a more normal scale as in scenario analysis. Stress testing generally is used as a complement to probabilistic measures to examine the results of low likelihood, high impact events that might not be captured adequately by distributional assumptions used with probabilistic techniques.

FIGURE 28  CMOL module with scenario analysis and stress testing
COSO Application Techniques, Exhibit 5.8-5.9: Loss Distributions, Back Testing, Sensitivity Analysis

Certain operational or credit loss distribution estimations use statistical techniques, generally based on non-normal distributions, to calculate maximum losses resulting from operational risks with a given confidence level. Back-testing [historical simulation] typically consists of periodic comparison of an entity’s at-risk measures with subsequent profit or loss. Back-testing commonly is used by financial institutions. Sensitivity analysis is used to assess the impact of normal, or routine, changes in potential events.

**FIGURE 29** CMOL module with historical simulation (back-testing) and Value at Risk