risk oversight solutions

A better response to risk.

RiskStatus*line*™ Quick Reference & Objective Centric ERM & Internal Audit Key Concepts

This document includes the RiskStatus*line*™ Quick Reference document which is an overview of key concepts to the Objective Centric ERM & Internal Audit methodology, as well as key concepts for implementation.

Implementing Objective Centric ERM & Internal Audit? Need help?

Call Risk Oversight Solutions or an authorized service provider today

Risk Oversight Solutions Inc. was established to help companies, boards, internal auditors, and risk specialists implement a dramatically better approach to ERM and internal audit - Objective Centric ERM & Internal Audit to meet new expectations.

Objective Centric ERM & Internal Audit has been specifically designed to focus the efforts of top management, work units and assurance groups on an organization's top value creation and preservation objectives – integrating the efforts of all assurance providers. The central goal is to generate better information on the true state of retained risk to help senior management and the Board make better resource allocation decisions and drive long term value creation and preservation. Using end result objectives as a foundation for integrated assurance is a simple step that quickly aligns strategic planning and the need to create and preserve long term value with the efforts of ERM and internal audit groups. Want a lot more value from your ERM and internal audit spending? Objective centric ERM and internal audit is the answer.

Our firm has over more than 30 years global experience helping company boards, senior management/workgroups, internal auditors and other assurance specialists implement more cost effective risk management and risk oversight frameworks. Objective Centric ERM & Internal Audit aligns with both COSO ERM and ISO 31000.

Call us today to start implementing Objective Centric ERM & Internal Audit.

www.riskoversightsolutions.com or info@riskoversightsolutions.com

RiskStatus*line*™ Quick Reference Sheet

BUSINESS OBJECTIVE FAMILIES

1. Product Quality (PQ)
2. Customer Service (CS)
3. Minimizing Unnecessary Costs (MUC)
4. Revenue/Profit Maximization (RPM)
5. Reliable Business Information (RBI)
6. Asset Safeguarding (AS)
7. Safety (S)
8. Regulatory Compliance (RC)
9. Fraud Prevention/Detection (FPD)
10. Continuity of Operations (COO)
11. Unintentional Risk Exposure (URE)
12. Contract Compliance (CC)
13. Internal Compliance (IC)

Note: The families sometimes overlap. The objective should be assigned to the family most descriptive of the objective type.

RISK SOURCES

- Commercial/Legal
- Competition
- Control Design
- Customers
- Employees
- Environmental Liability
- Equipment/Technology
- Finance/Economic
- Fraud/Corruption
- Human Behaviour
- Missing Objectives
- Natural Events
- Political Influences
- Product/Service Liability
- Public Perception
- Suppliers

RESIDUAL RISK STATUS INFORMATION

Indicator Data– Any information available about how well the objective is being achieved.

Impediment Data – Any situations or problems that stand in the way of the objective owner/sponsor adjusting the risk treatment strategy and related residual risk status. These can relate to the lack of funds, cooperation of staff or other departments, training deficiencies, board/senior management attitudes, and others.

Concern Data – Any known or suspected problems or concerns with one or more risk treatments/controls in place to manage risk likelihood and/or consequence. It can also include viable risk treatments available that are not currently selected.

Impact Data– How bad would it be if the objective was not met in whole or in part? How would the board, the organization, the staff, and others be impacted?

COMPOSITE RESIDUAL RISK RATING DEFINITIONS

0 Fully Acceptable – Composite residual risk status is acceptable. No changes to risk treatment strategy required at this time. (NOTE: this could mean that one or more significant risks are being accepted. Information on accepted concerns is found in the Residual Risk Status information)

1 Low - Inaction could result in very minor negative impacts. Ad hoc attention may be required to adjust composite residual risk status to an acceptable level.

2 Minor – Inaction or unacceptable terms could result in minor negative impacts. Routine management attention may be required to adjust composite residual risk status to an acceptable level.

3 Moderate - Inaction could result in or allow continuation of mid-level negative impacts. Moderate senior management effort required to adjust composite residual risk status to an acceptable level.

4 Advanced – Inaction could allow continuation of /or exposure to serious negative impacts. Senior management attention required to adjust composite residual risk status.

5 Significant - Inaction could result in or allow continuation of very serious entity level negative impacts. Senior management attention urgently required to adjust composite residual risk status to an acceptable level.

6 Major - Inaction could result in or allow continuation of very major entity level negative consequences. Analysis and corrective action to adjust composite residual risk status required immediately.

7 Critical - Inaction virtually certain to result in or allow continuation of very major entity level negative consequences. Analysis and corrective action to adjust composite residual risk status required immediately.

8 Severe - Inaction virtually certain to result in or allow continuation of very severe negative impacts. Senior management/board level attention urgently required to adjust composite residual risk status.

9 Catastrophic – Inaction could result in or allow the continuation of catastrophic proportion impacts. Senior management/board level attention urgently required to adjust composite residual risk status and avert a catastrophic negative impact on the organization.

10 Terminal - The current composite residual risk status is already extremely material and negative and having disastrous impact on the organization. Immediate top priority action from the board and senior management required to prevent the demise of the entity.

RiskStatus*line*™ Risk Treatment Elements

1. PURPOSE: DEFINITION & COMMUNICATION
1.1 Definition of Corporate Mission & Vision
1.2 Definition of Entity Wide Objectives
1.3 Definition of Unit Level Objectives
1.4 Definition of Activity Level Objectives
1.5 Communication of Business/Quality Objectives
1.6 Definition and Communication of Corporate Conduct Values and Standards

2. COMMITMENT
2.1 Accountability/Responsibility Mechanisms
2.1a Job Descriptions
2.1b Performance Contracts/Evaluation Criteria
2.1c Budgeting/Forecasting Processing
2.1d Written Accountability Acknowledgements
2.1e Other Accountability/Responsibility Mechanisms
2.2 Motivation/Reward/Punishment Mechanisms
2.2a Performance Evaluation System
2.2b Promotion Practices
2.2c Firing and Discipline Practices
2.2d Reward Systems - Monetary
2.2e Reward Systems - Non-Monetary
2.3 Organization Design
2.4 Self-Assessment/Risk Acceptance Processes
2.5 Officer/Board Level Review
2.6 Other Commitment Controls

3. PLANNING & RISK ASSESSMENT
3.1 Strategic Business Analysis
3.2 Short, Medium and Long Range Planning
3.3 Risk Assessment Processes - Macro Level
3.4 Risk Assessment Processes - Micro Level
3.5 Control & Risk Self-Assessment
3.6 Continuous Improvement & Analysis Tools
3.7 Systems Development Methodologies
3.8 Disaster Recovery/Contingency Planning
3.9 Other Planning & Risk Assessment Processes

4. CAPABILITY/CONTINUOUS LEARNING
4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes
4.2 Self-Assessment Forums & Tools
4.3 Coaching/Training Activities & Processes
4.4 Hiring and Selection Procedures
4.5 Performance Evaluation
4.6 Career Planning Processes
4.7 Firing Practices
4.8 Reference Aids
4.9 Other Training/Education Methods

5. DIRECT CONTROLS
5.1 Direct Controls Related to Business Systems
5.2 Physical Safeguarding Mechanisms
5.3 Reconciliations/Comparisons/Edits
5.4 Validity/Existence Tests
5.5 Restricted Access
5.6 Form/Equipment Design
5.7 Segregation of Duties
5.8 Code of Accounts Structure
5.9 Other Direct Control Methods, Procedures, or Things

6. INDICATOR/MEASUREMENT
6.1 Results & Status Reports/Reviews
6.2 Analysis: Statistical/Financial/Competitive
6.3 Self-Assessments/Direct Report Audits
6.4 Benchmarking Tools/Processes
6.5 Customer Survey Tools/Processes
6.6 Automated Monitoring/Reporting Mechanisms & Reports
6.7 Integrity Concerns Reporting Mechanisms
6.8 Employee/Supervisor Observation
6.9 Other Indicator/Measurement Controls

7. EMPLOYEE WELL-BEING & MORALE
7.1 Employee Surveys
7.2 Employee Focus Groups
7.3 Employee Question/Answer Vehicles
7.4 Management Communication Processes
7.5 Personal and Career Planning
7.6 Diversity Training/Recognition
7.7 Equity Analysis Processes
7.8 Measurement Tools/Processes
7.9 Other Well-Being/Morale Processes

8. RISK SHARING/TRANSFER
8.1 Insurance Coverage
8.2 Contractual Indemnities/Remediation
8.3 Civil Law Recovery
8.4 Other Risk Sharing/Transfer Vehicles

9. RISK OVERSIGHT
9.1 Manager/Officer Monitoring/Supervision
9.2 Internal Audits
9.3 External Audits
9.4 Specialist Reviews & Audits
9.5 ISO Review/Regulator Inspections
9.6 Audit Committee/Board Oversight
9.7 Self-Assessment Quality Assurance Reviews
9.8 Authority Grids/Structures & Procedures
9.9 Other Risk Oversight Activities

Objective Centric ERM & Internal Audit: Key Concepts

POPULATING THE OBJECTIVES REGISTER:

1. Tradeoff between the cost of formal demonstrable assurance versus potential benefits
2. Relevance of the objectives to board/senior execs
3. Should include top "value creation" objectives and top " value preservation/erosion" objectives
4. Top value creation objectives should integrate with the organization's top strategic objectives
5. Regulator expectations of what objectives/areas should be covered by formal assurance processes
6. What's in the OBJECTIVES REGISTER should drive the work of all assurance specialists
7. All objectives in the REGISTER should have an OWNER/SPONSOR

PRIORITIZING OBJECTIVES IN THE REGISTER:

1. Value creation ability – entity level
2. Potential to erode value – entity level
3. Importance to company/board
4. Importance to Owner/Sponsor of the objective
5. Current and target performance level gaps
6. Link to executive remuneration targets
7. What regulators think is important at a point in time (e.g. FCPA, AML, insider trading)
8. Priority of specific objectives on the board's agenda
9. Current public profile/media exposure
10. Expectations of external auditor/customers

COMPOSITE RESIDUAL RISK RATINGS: ("CRRRs")

1. CRRRs scale is set at the entity level to provide "fit for purpose" information for C-Suites and boards
2. Focus is on deciding on appropriate residual risk status escalation level (i.e. unit management/senior management/board)
3. Goal is to produce concise and relevant consolidated reports for senior management and the board on the objectives in the OBJECTIVES REGISTER currently rated as being outside the organization's risk appetite/tolerance by OWNER/SPONSOR and/or Internal Audit
4. All items with CRRR of 1 or greater indicates that the current status for that objective is outside of corporate risk appetite. How far outside, and how dangerous the status, is communicated by higher CRRR values.
5. When the CRRR = 0 means residual risk status for that objective is deemed fully acceptable to senior management. It does not mean there is zero retained/residual risk for that objective
6. In this system CRRR ratings of 1 or greater must have an action plan. If no new/different risk treatments it should be 0
7. Generally, CRRRs of 4 or greater warrant particular board attention

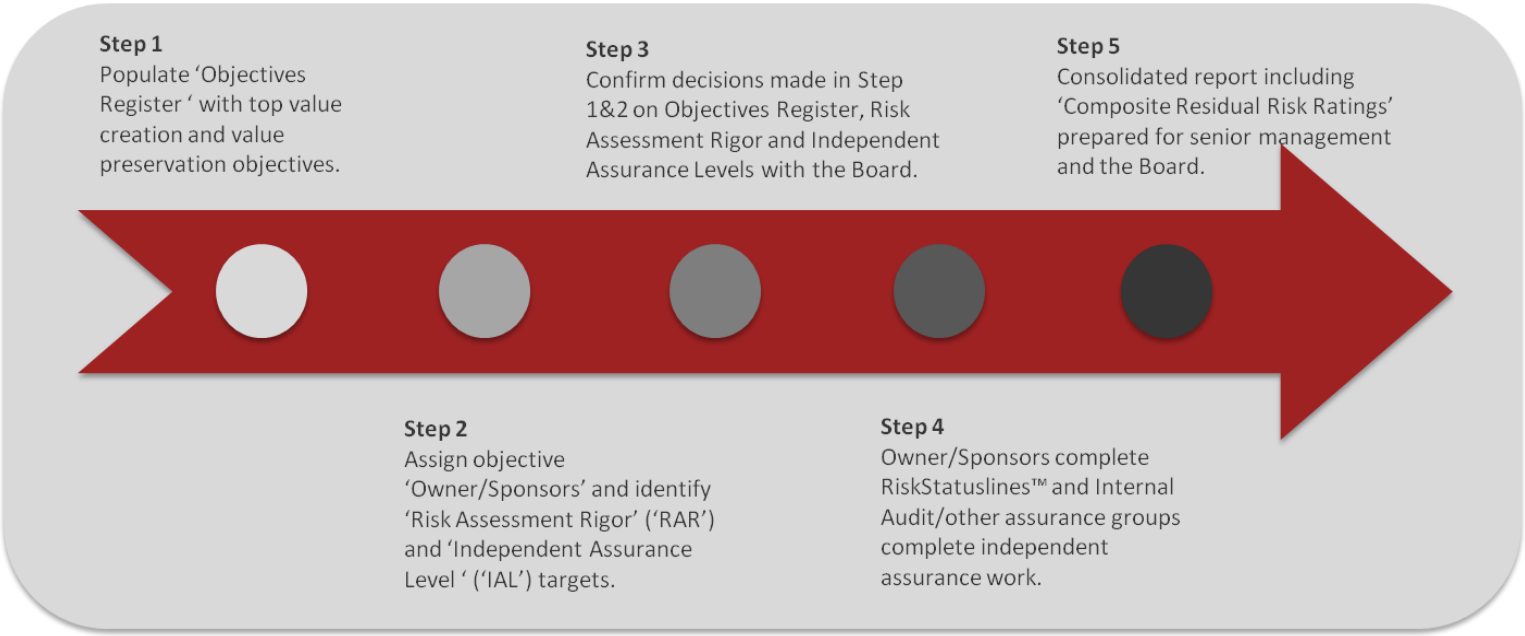
RISK ASSESSMENT RIGOUR/RIGOR ("RAR")

1. Boards should be told the level of assessment rigor (the amount of formal risk assessment effort) applied to each objective – they often have not been told the level of rigor applied by ERM teams/Internal Audit/Management
2. Higher rigor generally should result in higher data reliability however higher rigor comes with higher costs
3. A large % of traditional risk register assessments historically have been done with relatively low rigor
4. A large % of traditional IA work historically has been done with generally low focus/time spent on risk identification and assessment and high focus/time spent on "controls", a subset of available risk treatments.
5. A large % of traditional ERM and IA work has not linked conclusions on control "effectiveness" to the impact of non-achievement of key objectives, performance levels, or provided information on viable risk treatments not used/applied
6. "Brain-storming" has often been the only risk identification method used by IA and ERM groups. History indicates, in isolation, it is often unreliable

INDEPENDENT ASSURANCE LEVEL ("IAL")

1. Boards should be told the independent assurance level attached to risk/control reports they receive – often they are not
2. Boards should take responsibility for defining how much independent assurance they want on the risk status information they want/ receive. The FRC in the UK has codified this as a formal board oversight expectation.
3. Higher independent assurance on information should, on balance, equal higher reliability.
4. Independent assurance costs money. The cost of independent assurance should be transparent and decided consciously by boards and management – i.e. it should be demand driven and consciously determined
5. Boards should want some level of independent assurance on the risk status of top value creation objectives, as well as top value erosion objectives

Objective Centric ERM & Internal Audit: Key Concepts



Risk Assessment Rigour ("RAR") Levels

RAR	DESCRIPTION
Not Assigned (NA)	Accountability to report on the Composite Residual Risk Rating ("CRRR") has not been assigned to an OWNER/SPONSOR(s)
Not Rated (NR)	Accountability has been assigned to an OWNER/SPONSOR(s) but no CRRR has been assigned yet
Very Low (VL)	Accountability to report CRRR status has been assigned and a CRRR rating with a brief narrative explaining the basis for the CRRR provided by the objective OWNER/SPONSOR(s) within the past 12 months
Low (L)	A time-limited effort has been made to develop or update a list of risks/threats to achievement and assign RED/AMBER/GREENS to each risk within the past 12 months. Action items for all RED rated risks will be developed
Medium (M)	More effort has been spent to quality assure that all significant risks have been identified using a variety of risk identification methods and the risk treatments in place/use for all, or some, of the risks have been identified and documented. Performance and impact information for the objective has been obtained and documented. Data has been updated within the past 12 months.
High (H)	A range of techniques have been used to identify all significant risks. Risk treatments for significant risks have been identified and efforts made to independently validate the existence and effectiveness of the risk treatments. Efforts have been made to validate the adequacy and accuracy of the linked objective performance and impact information.
Very High (VH)	All standard RiskStatusline™ information elements have been identified and documented and additional efforts made by the OWNER/SPONSOR(s) to validate their completeness and reliability.
Very High + (VH+)	In addition to identifying and documenting all standard RiskStatusline™ data elements, more advanced techniques to determine velocity of risks, leading/lagging risk indicators, steps taken to assess the reliability of likelihood and consequence ratings and other advanced risk assessment techniques

Independent Assurance ("IA") Levels

IA	DESCRIPTION
NIA	No independent assurance
LOW	A high level independent assurance review has been completed and a feedback report provided to the OWNER/SPONSOR and RISK OVERSIGHT COMMITTEE
MEDIUM	An independent review has been completed to assess the completeness of risks identified, risk treatments, and residual risk status information and a report provided to the objective's OWNER/SPONSOR and the RISK OVERSIGHT COMMITTEE
HIGH	In addition to the steps defined for MEDIUM, steps have been taken to independently confirm the existence and effectiveness of the risk treatments identified.