



A better response to risk.

RiskStatusline™ Risk Treatment Principles Diagram and Trigger Statements

This document provides the Risk Treatment Principles overview diagram and the expanded trigger statements when considering risk treatments.

Risk Oversight Solutions offers the following reference aid to public and private sector organizations free of charge, with the exception of any organization whose purpose is to generate revenue from direct or indirect sale of the materials. Contact us today to become an authorized distributor. Permission to reproduce with attribution is granted by Risk Oversight Solutions Inc. (ROS), with the exception noted above.

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

RiskStatusline™

Risk Treatment Principles

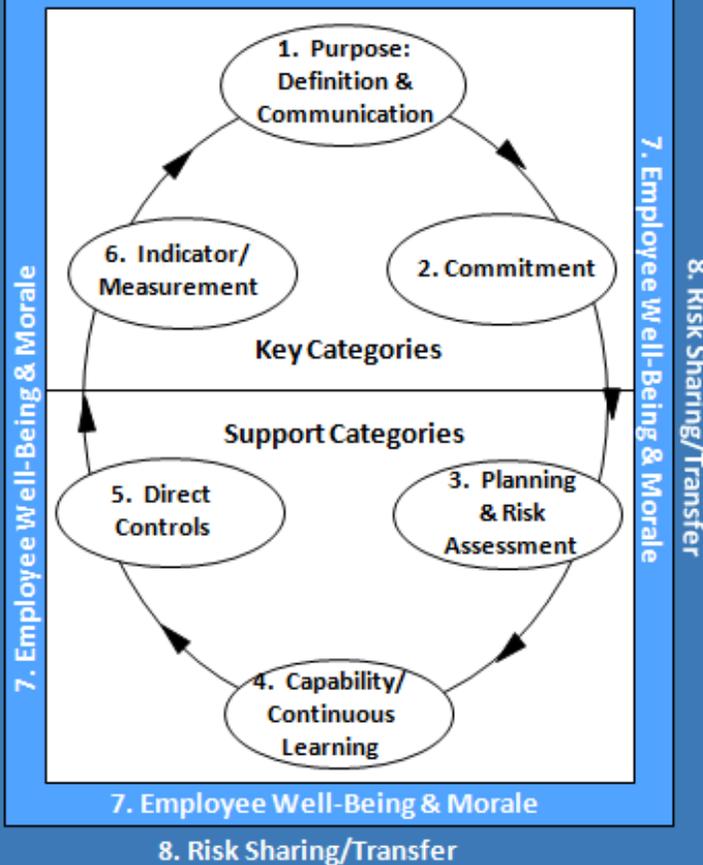
1. Purpose - Definition & Communication: Do we know the end result objectives we must achieve to be successful? Have we formally defined and communicated them to the people that need to support them?

2. Commitment: Are the people that are important to the achievement of specific objectives committed to the achievement of those objectives?

9. Risk Oversight

8. Risk Sharing/Transfer

7. Employee Well-Being & Morale



3. Planning & Risk Assessment: Are we thinking about what lies ahead and the barriers and obstacles we may have to deal with? Have we considered how we will deal with risks that threaten objectives?

4. Capability/Continuous Learning: Do we have the necessary knowledge and skills to achieve our objectives?

5. Direct Controls: What specific methods, procedures or devices help directly assure the achievement of our objectives?

6. Indicator/Measurement: Do we know how well we are, or are not, achieving our objectives?

7. Employee Well-Being & Morale: Is employee well-being and morale negatively or positively impacting on the achievement of objectives?

9. Risk Oversight: Are there people and processes in place to oversee that the risk treatments are resulting in an acceptable level of residual risk (i.e. in-line with our risk appetite/tolerance)?

8. Risk Sharing/Transfer: Do we have insurance coverage or contractual terms and indemnities in place to manage risks to our objectives?

RiskStatusline™ Risk Treatment Elements

Trigger Statements

1.0 PURPOSE: DEFINITION & COMMUNICATION

Primary Category Definition: Do we know the end result business objectives we must achieve to be successful? Have we formally defined and communicated these to the people that need to support them?

1.1 Definition of Corporate Mission & Vision

- The organization has defined its primary reason for existence.
- The organization has a documented mission and/or vision statement.

1.2 Definition of Entity Level Objectives

- The organization has defined the key end result business objectives that it needs to accomplish.
- They can include objectives related to customer service, product quality, cost control, revenue generation, fraud prevention, reliable business information, legal/regulatory compliance, and others.

1.3 Definition of Unit Level Objectives

- End result business objectives have been defined for each business unit or team.
- These are linked to the objectives defined in elements 1.1 and 1.2.
- There is a process to check that unit and activity level objectives support corporate level objectives.

1.4 Definition of Activity Level Objectives

- End result business objectives are clearly defined for, or linked to, all activities being carried out in the business units.
- People know what they are expected to do, and more importantly, why they are doing these activities.

1.5 Communication of Business Objectives

- End result business objectives been communicated to all the people that must support the achievement of those objectives.
- They understand what the objectives mean.

1.6 Definition and Communication of Corporate Conduct Values and Standards

- Specifically in the area of objectives related to corporate conduct and ethics, the organization has communicated its values and standards to employees, suppliers, customers and other relevant stakeholders.
- There is a process to update and communicate these standards regularly.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

2.0 COMMITMENT

Primary Category Definition: Are the people that are important to the achievement of specific objectives committed to the achievement of those objectives?

2.1 Accountability/Responsibility Mechanisms

- The organization or unit has defined and assigned accountability for achieving end result business objectives. (Note: it is important to distinguish between assigning accountability for completion of activities or processes versus defining accountability for end result business objectives).

2.1a Job Descriptions

- Employees know through job descriptions or other documentation the specific end result business objectives their daily work supports.

2.1b Performance Contracts/Evaluation Criteria

- Performance contracts or other forms of employee evaluation criteria are linked to specific end result business objectives (i.e. performance evaluation is linked to specific end result business objectives).

2.1c Budgeting/Forecasting Processing

- The budget and forecasting process links the achievement of objectives to specific business units and/or individuals.

2.1d Written Accountability Acknowledgements

- Employees have been asked to formally acknowledge in some way that they accept responsibility for one or more end result business objectives.

2.1e Other Accountability/Responsibility Mechanisms

- There are other mechanisms which establish accountability for specific end result business objectives.

2.2 Motivation/Reward/Punishment Mechanisms

- There are personal consequences related to the accomplishment or non-accomplishment of specific end result business objectives.

2.2a Performance Evaluation System

- There are clear linkages between publicized end result business objectives and the employee performance evaluation system(s) in use.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

2.2b Promotion Practices

- There is linkage between the organization's stated objectives and the performance of those that are being promoted or demoted.

2.2c Firing and Discipline Practices

- There are negative consequences attached to lack of commitment to end result business objectives up to and including firing of those responsible for supporting the achievement of those objectives.

2.2d Reward Systems - Monetary

- There is visible linkage between the accomplishment of specific objectives and the monetary rewards provided by the organization.

2.2e Reward Systems - Non-Monetary

- There are non-monetary techniques or methods that provide positive consequences for achievement of business objectives, or negative consequences for the non-achievement of the objectives (e.g. employee or team awards, special recognition, plaques, posters showing units that are not meeting targets, etc.).

2.3 Organization Design

- The design of the organization and sub units assists in clarifying who is responsible and/or accountable for specific end result business objectives.

2.4 Self-Assessment/Risk Acceptance Processes

- Work units engage in self-assessment processes which assist in clarifying and/or reinforcing ownership of end result business objectives.

2.5 Officer/Board Level Review

- Senior management and/or the board of directors ask for information and reports on specific end result business objectives and/or the adequacy of the systems and processes that support the achievement of those objectives.

2.6 Other Commitment Controls

- There are other mechanisms in use or place which increase the commitment of employees to achieve end result business objectives.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

3.0 PLANNING & RISK ASSESSMENT

Primary Category Definition: Are we thinking about what lies ahead and the barriers and obstacles we may have to deal with? Have we considered how we will deal with risks that threaten objectives?

3.1 Strategic Business Analysis

- The organization periodically analyzes the current level of achievement relative to what the organization believes should or must be accomplished.

3.2 Short, Medium and Long Range Planning

- The organization plans for the immediate future, usually covering the next year, the medium term often viewed as a two to five year time horizon, and the longer term which may stretch out decades.

3.3 Risk Assessment Processes - Macro Level

- There are mechanisms or forums to identify, consider and analyze the significant risks which may threaten the achievement of the organization's end result business objectives, including risks related to inadequate human and/or monetary resources.

3.4 Risk Assessment Processes - Micro Level

- There are mechanisms or processes in place to analyze specific risks or threats which may result in the non-achievement of end result business objectives of specific departments, business units or other part of the entity, including risks caused by inadequate or inappropriate human, monetary or other resources.

3.5 Risk Self-Assessment

- Work units or groups of employees with responsibility for specific end result business objectives periodically take time to develop or clarify objectives, formally analyze the risks or threats to their objectives, and assess the ability of the risk treatments in use or place to mitigate these threats.

3.6 Continuous Improvement & Analysis Tools

- The organization and/or sub units use formalized techniques to continuously review and improve work methods and processes (e.g. total quality management tools, recognized quality systems such as Six Sigma, Malcolm Baldrige, European Quality Model, ISO 9000 series of standards, etc).

RiskStatusline™ Risk Treatment Elements

Trigger Statements

3.7 Systems Development Methodologies

- The organization uses some form of structured development method when designing or reengineering business systems products or processes that specifies end result objectives sought and considers possible threats and obstacles to the achievement of objectives.

3.8 Disaster Recovery/Contingency Planning

- The organization has mechanisms or processes in place to anticipate and consider the possibility of significant negative and/or positive events and develop plans to deal with these situations. Examples include disasters, cyber attacks, executive kidnapping, terrorist attacks, major natural disasters, a hugely successful sales launch that overwhelms resources, demise of a competitor, new technology, negative or positive legislative developments, and others.

3.9 Other Planning & Risk Assessment Processes

- There are other processes or activities that relate to the analysis of the past, consideration of threats and opportunities that may occur in the future, and establishment of plans to achieve end result business objectives.

4.0 CAPABILITY/CONTINUOUS LEARNING

Primary Category Definition: Do we have the necessary knowledge and skills to achieve our objectives?

4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes

- There are processes in place to define the knowledge levels and skills necessary to successfully meet job responsibilities and achieve objectives; inventory the knowledge and skills of the people doing the work or being considered for job assignments, and frameworks or processes to close any knowledge/skill gaps identified.

4.2 Self-Assessment Forums & Tools

- A process exists for people individually or collectively to take time to consider whether their current knowledge levels, skill sets, and resource levels are adequate to achieve the organization's end result business objectives.

4.3 Coaching/Training Activities & Processes

- There are processes in place to close knowledge or skill gaps through coaching and/or other forms of training activities. These can be informal methods such as on the job coaching and feedback, or involve more formalized training in classroom or workshop environments.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

4.4 Hiring and Selection Procedures

- The hiring and selection process formally considers the knowledge and skill attributes of candidates and attempts to hire or select personnel that have knowledge and skill profiles as close to the desired knowledge and skill profile as is possible. Or alternatively, if knowledge and skill mismatches are accepted consciously, steps are taken to mitigate the risks that may result.

4.5 Performance Evaluation

- The performance evaluation process in use attempts to identify and correct performance related problems which are being caused by knowledge and/or skills gaps.

4.6 Career Planning Processes

- The organization has formalized processes to identify the developmental steps necessary to ensure employees are acquiring knowledge, skill and experience necessary to fill positions that may open up or emerge in the organization in the future.

4.7 Firing Practices

- When serious efforts have been made to correct knowledge and skill gaps but the efforts have been unsuccessful, the organization takes steps to address capability and/or commitment problems through termination or job reassignment.

4.8 Reference Aids

- There are reference aids or resources available which employees can refer to assist them in fulfilling their job responsibilities.

4.9 Other Training/Education Methods

- There are other processes or activities which increase the assurance that people have the necessary knowledge and skill.

5.0 DIRECT CONTROLS

Primary Category Definition: What specific methods, procedures or devices help directly assure the achievement of our objectives?

5.1 Direct Controls/Risk Treatments Related to Business Systems

- There are specific direct controls/risk treatments built in to business systems to ensure the desired results are achieved. (Note: these tend to be the type of “controls” auditors have historically concentrated on when evaluating control systems).

RiskStatusline™ Risk Treatment Elements

Trigger Statements

5.2 Physical Safeguarding Mechanisms

- There are risk treatments which protect the organization's assets through direct measures such as locks on doors, bars on windows, use of safes to secure valuables, fences around the perimeter of a plant, armed guards protecting a work site, and other similar techniques.

5.3 Reconciliations/Comparisons/Edits

- There are traditional risk treatment techniques such as reconciling bank accounts, comparisons of subledger totals to control accounts, system edits, etc. that are relevant to the achievement of the objective.

5.4 Validity/Existence Tests

- There are mechanisms to validate the existence of assets. Fairly common examples include physical inventory counts to determine that quantities and descriptions of goods and/or supplies on hand are accurate, fixed asset inventories to validate the existence of items represented in the accounts, and other similar processes.

5.5 Restricted Access

- Data is in manual files or computer stored records protected from unauthorized access through systems based or manual techniques.

5.6 Form/Equipment Design

- The design of manual business forms, computer input screens, or equipment such as cash registers or computer input terminals assist to reduce the probability of errors.

5.7 Segregation of Duties

- Tasks or processes are segregated to reduce the risk of accidental errors and/or fraud.

5.8 Code of Accounts Structure

- The design of the general ledger or subledger account codes assist in minimizing errors and allow for effective data capture and reporting.

5.9 Other Direct Control Methods, Procedures, or Things

- There are other methods, procedures or things that have a direct impact on ensuring the achievement of business/quality objectives.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

6.0 INDICATOR/MEASUREMENT

Primary Category Definition: Do we know how well we are, or are not, achieving our objectives?

6.1 Results & Status Reports/Reviews

- There are processes or other mechanisms in use or place which report on or examine the achievement status of a particular end result business objective or objectives. A common example is the review of the monthly or quarterly financial results by senior management or the board against targets. Other examples include a safety review meeting, environmental status review, customer service level reports, and many others.

6.2 Analysis: Statistical/Financial/Competitive

- There are analysis processes in place or use that analyze current achievement levels against relevant benchmarks or planned achievement levels.

6.3 Self-Assessments/Direct Report Audits

- There are self-assessment activities which include specific consideration of how well an end result business objective is, or is not being achieved. There are audits performed by people not responsible for the activity or objective which examine and consider the current achievement status relative to some desired or required status.

6.4 Benchmarking Tools/Processes

- The organization benchmarks current achievement levels against the levels or outputs achieved by others. Common examples include benchmarking the cost to produce a defined product or service relative to that of others, comparing service levels provided relative to competitors, performance of a fund manager compared to that of other fund managers, and many other applications.

6.5 Customer Survey Tools/Processes

- There are activities and processes that seek information and feedback from customers in relation to a business/quality objective or objectives. These processes may be very sophisticated and intensive, or as simple as a customer complaint hotline.

6.6 Automated Monitoring/Reporting Mechanisms & Reports

- There are measurement activities undertaken by computers or machines which result in action occurring if the mechanism indicates situations outside of acceptable tolerance.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

6.7 Integrity Concerns Reporting Mechanisms

- There are reporting options in place that allow people to report situations which are, or may be, violations of corporate ethical standards or societal objectives without fear of reprisal. Integrity concerns relate to areas such as employee or corporate honesty, individual or corporate compliance with the law, treatment of people, and other similar situations. These are also referred to as hotlines, or whistleblowing options.

6.8 Employee/Supervisor Observation

- Employees and/or supervisors observe directly the current status of achievement related to one or more end result business objectives. This can include a service supervisor observing the length of a line-up for bank services, a construction worker assessing if a pipeline is being built to the required specifications, an employee spotting a flawed product being loaded for shipment, etc.

6.9 Other Indicator/Measurement Controls

- There are other methods, procedures or other things that assist in determining how well or how badly a specified end result business objective is, or is not being achieved.

7.0 EMPLOYEE WELL-BEING & MORALE

Primary Category Definition: Is employee well-being and morale negatively or positively impacting on the achievement of objectives.

7.1 Employee Surveys

- Employees are periodically surveyed to determine their views and attitudes to the organization. Employees view the organization as a good or a bad place to work. They believe that the organization treats employees fairly and with respect.

7.2 Employee Focus Groups

- The organization periodically assembles groups of employees to discuss and obtain feedback on issues important to the success of the organization. The organization works to create shared visions of what is important and the direction it is taking to succeed.

7.3 Employee Question/Answer Vehicles

- Management at all levels provide opportunities for employees to ask questions regarding the organization's direction, treatment of employees, ethical values, and other areas of employee concern or interest.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

7.4 Management Communication Processes

- Management personnel at all levels are encouraged and trained to effectively communicate with employees in their business units. There are mechanisms in place to identify managers that are weak in this skill area. The organization has vehicles such as company web site, e-mail, newsletters, communication hotlines, etc. that provide mechanisms which encourage frank and candid communication with staff.

7.5 Personal and Career Planning

- There are mechanisms and processes in place which assist employees to think about their careers and consider ways to develop and achieve their personal work related goals. The organization provides management training or specialist assistance to help employees identify sources of help and guidance when they are having severe difficulties in their personal lives such as alcohol or drug dependencies, death of close family members, divorce, severe depression, etc.

7.6 Diversity Training/Recognition

- Managers and employees at all levels are provided with awareness training, and if necessary, behaviour modification coaching, to ensure that they understand the value of diversity in the composition of work teams and organizations.

7.7 Equity Analysis Processes

- The organization or work units periodically take time to self-assess or have other mechanisms to assess whether employees are being treated fairly in terms of pay, opportunities and other relevant areas.

7.8 Measurement Tools/Processes

- The organization attempts to measure and track the state of morale in the organization and in the various business units that make it up to identify problems which may seriously impact on the organization's ability to achieve its objectives.

7.9 Other Well-Being/Morale Processes

- There are other methods, procedures or other things which assist in measuring and improving employee morale.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

8.0 RISK SHARING/TRANSFER/FINANCE

Primary Category Definition: Do we have insurance coverage and/or contractual terms and indemnities in place to manage risks to our objectives?

8.1 Insurance Coverage

- The organization assesses risks and makes careful decisions when it makes economic sense to acquire insurance coverage that will mitigate the impact of specified risks in the event other risk treatment strategies, if any, allow specified risks to negatively impact the organization. (NOTE: It is very important to identify what specifically the insurance covers, deductibles, and any exclusions)

8.2 Contractual Indemnities/Remediation

- Contracts with customers, suppliers, and others contain clauses/provisions that specify responsibility of the parties to the contract and remedies in the event of certain specified situations and/or risks occurring.

8.3 Civil/Criminal Law Recovery

- In cases where a risk has resulted in financial, reputational or other forms of damage, the organization pursues steps to mitigate the damages sustained through criminal and/or civil remedy channels.

8.4 Other Risk Sharing/Transfer/Finance Vehicles

- Other methods, procedures, or other things which mitigate the likelihood and/or consequences of one or more risks through the use of some form of risk sharing/transfer/finance vehicle.

9.0 RISK OVERSIGHT

Primary Category Definition: There are people or processes in place to check that the risk treatments in use/place are resulting in an acceptable level of residual risk (i.e. current composite risk/uncertainty of not achieving objectives).

9.1 Manager/Officer Monitoring/Supervision

- Managers at all levels periodically assess the areas they are responsible for to determine if the current risk treatment mechanisms and strategies in place are resulting in an acceptable level of residual risk. Managers and officers demonstrate that the risk treatments in use or place are conscious selections that have been arrived at after careful consideration of the relevant risks.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

9.2 Internal Audits

- Internal audit personnel periodically review specified topics or business areas to analyze whether the risk treatments in use/place are cost effective and resulting in a level of assurance and residual risk that is acceptable to the work unit, senior management and the board of directors (e.g. internal auditors, safety auditors, environmental auditors, quality auditors, etc.).

9.3 External Audits

- Personnel external to the organization are used to assess and report on the organization's public disclosures particularly those related to the organization's financial status.

9.4 Specialist Reviews & Audits

- The organization engages specialists from time to time to examine and report on the way the organization is managing specific issues or areas of business activity. These reviews can relate to any facet of an organization's activities including such things as customer service, product quality, cost minimization, safety, fraud prevention, regulatory compliance, computer security, derivatives trading operations, and others.

9.5 ISO Review/Regulator Inspections

- The organization periodically measures its business methods and frameworks against known risk, control or quality criteria such as: the ISO 9000 and 14000 series of standards; ISO 31000 risk management standard, quality frameworks including the Malcolm Baldrige system, European Quality Foundation model, derivatives of the Baldrige systems; a disclosed control framework such as COSO 1991, COSO 2012, COCO, the RiskStatusline™ risk treatment principles, or regulatory criteria related to specific industries or areas of business activity.

9.6 Audit Committee/Board Oversight

- The audit committee and the board of directors as a whole understand and fulfill their responsibility to oversee the adequacy of the risk management frameworks established by management. The board has subjected the quality of their risk oversight to a self-assessment process or an external review to check if they are measuring up to national and/or international governance best practices such as the NACD risk oversight guidance or the Canadian standards for directors related to board risk oversight. There is evidence that the board of directors is asking for, and receiving, the quantity and quality of information on the status of risk management processes and residual risk status necessary to meet their risk oversight and governance responsibilities.

9.7 Self-Assessment Quality Assurance Reviews

- The organization utilizes self-assessment processes to examine and report on all or part of the operation, and the self-assessment reports are subjected to some form of quality assurance review to ensure that they are producing reliable information.

RiskStatusline™ Risk Treatment Elements

Trigger Statements

9.8 Authority Grids/Structures & Procedures

- The organization has formalized criteria that specifies the level of management, up to and including the board of directors that must review and approve decisions taken or being considered by employees and management in the business units. Authority grids may exist which relate to acceptable levels or residual risk, capital spending, hiring of senior executives, risk exposure positions related to derivatives or foreign currency movement, decisions to undertake new lines of business, geographic expansion plans, access to computer systems and files, and many others.

9.9 Other Process Oversight Activities

- There are other methods, procedures or other activities which are designed to assess the appropriateness of the control and risk management frameworks in place or in use in the organization.