Risk Oversight Solutions: Ten Primary Assurance Methods

AN OVERVIEW OF THE TEN METHODS

Section Objective:

Introduce participants to the ten primary assurance methods and their linkages (or lack thereof) to risks that create uncertainty objectives will be achieved.

There are five primary assurance methods. (See overview diagram at the end of this section) These methods can be done by auditors or other specialists using the "direct report" method of auditing (i.e. where auditors/other specialists are the primary analysts/reporters), or via a self-assessment approach (i.e. work unit/self-assessment group/management is the primary analyst/reporter). When self-assessment methods are used the self-assessment results may, or may not, be subjected to an independent quality assurance review. Since there are 5 direct report methods and 5 primary self-assessment methods this means that there are 10 primary assurance methods in total. Many variations of each method exist and are used in practice.

INTRODUCTION

The main assessment methods include:

Compliance-Centric – in this approach one or more auditors or management represented by one or more people involved in the work area evaluates the extent to which the group or organization, does, or does not, conform to a corporate policy requirement, rule, law, "control objective", audit guide requirement, etc. The method or methods used by the author of the compliance checklist to define the compliance rules/requirements is often not clear or disclosed. Checklist requirements are often not the product of a formal risk assessment that includes identifying and assessing likelihood and consequence of specific risks. The linkage to risks and end result business objectives is often not disclosed and explained to the people completing the compliance assessment.

Control-Centric – in this approach a self-assessment team or one or more auditors evaluates the extent to which the group or organization conforms to, or demonstrates, elements in a specific recognized control model/framework. (e.g. COSO internal control framework 2013, Risk Oversight Solutions Risk Treatment Principles and elements, checklists developed internally or by an external auditor) This approach does not include specific risks. The success of this approach is heavily dependent on the predictive ability of the framework selected for use. None of the main control frameworks including COSO Internal Control Framework 2013 or the Risk Oversight Solutions Risk Treatment Principles and Elements (see visual of principles and elements later in this section) have been empirically validated in terms of their ability to predict major governance failures.

Risk Oversight Solutions: Ten Primary Assurance Methods

Process-Centric – in this approach a self-assessment team or one or more auditors completes an assessment of one or more business processes and forms an opinion on the adequacy or effectiveness of the controls in place/processes. The emphasis on defining specific process objectives, risks to objectives, and linking risks identified to "risk treatments" is highly variable. Risks are rarely formally evaluated in terms of likelihood and consequences. Work units sometimes undertake process centric analysis, usually as part of a formal quality initiative.

Risk-Centric – in this approach management, a self assessment team, or one or more auditors identifies a "context", which could be the entire organization, a sub-unit, a topic, an area of interest, a collection of objectives or other contexts, and then identifies risks that could impact on that context, and controls, "risk treatments" (ISO 31000) or "risk responses" (COSO ERM) that mitigate risks. This approach often focuses heavily on "risk mitigation", better known as internal controls, and may or may not, identify other "risk treatment" strategies in place/use including risk transfer/share/finance options. "Brainstorming" is often the dominant method used to identify risks. In some organizations "risk registers" are established and risk owners assigned. "Heat maps" displaying risks identified are often used to report to senior management and the board. The concept of "risk owners" is widely promoted. See Risk Oversight Solutions white paper, The High Cost Of ERM Herd Mentality published by the London School of Economics Center for Analysis of Risk and Regulation (CARR) available at http://riskoversightsolutions.com/wp-content/uploads/2011/10/Risk-Oversight-The-High-Cost-of-Herd-Mentality-Tim-Leech-CARR-December-2012.pdf or the Risk Oversight Solution presentation contrasting objective centric vs risk centric methods available at http://riskoversightsolutions.com/wp-content/uploads/2011/03/Risk-Oversight-Solutions-Tim-Leech-Objective-Centric-vs-Risk-Centric-ERM-Risk-Spotlight-Webinar-March-23-2015.pdf for more details.

Objective-Centric – in this approach management , a self-assessment team, or one or more auditors or other specialists depending on whether the approach is direct report of self-assessment selects an end-result business objective, ideally a top strategic value creation or preservation objective, considers the internal and external context that objective must be achieved in, identifies and assesses risks that impact on the certainty the end result objective will be achieved, identifies the "risk treatments" or "risk responses" currently in place/use, and identifies the residual risk status – a composite set of information designed to help the owner/sponsor of the objective decide whether the current risk treatment strategy and level of "certainty" related to the achievement of the objective is, or is not, acceptable given the organization's risk appetite/tolerance. The Risk Oversight Solutions approach to objective centric assessment is called "RiskStatusline". It is the only methodology that focuses on painting a picture of the current "Residual Risk Status" and includes a direct link to best available information on the current performance being achieved for the objective being assessed. Other variations exist. In the Risk Oversight Solutions approach primary assignment of responsibility for risk management is assigned to one or more "Owner/Sponsors". A universe of business objectives covering all important dimensions of the organization is created, owner/sponsors assigned and the status of risk assessment work done and residual risk status is tracked and reported upwards.

COMPLIANCE-CENTRIC APPROACH

STEP 1 Select the business entity, area or topic for assessment.

STEP 2 Select the corporate policy components or laws and/or regulations that you want information on from work units or senior management. This can be simply the degree that the work unit is, or is not, following corporate policies or involve the use of extensive audit checklists.

This information is then usually converted to a series of questions that the auditors or work unit and/or relevant individuals must answer.

Traditionally compliance self-assessment has been paper based or captured as a computer file. The same compliance assessment activities can now be done via an intranet or the internet.

STEP 3 Develop instructions or guidance for the recipients to use when responding to the assessment questions.

This is particularly important when the questions or issues do not lend themselves to simple answers and/or when attempting to use a standardized scale to get responses on a range of issues:

EXAMPLE #1
Has the unit complied with the obligation to obtain and submit Code of Conduct receipt confirmation and compliance declarations to Human Resources?

YES _____ NO _____ PARTIALLY _____

EXAMPLE #2
Background checks are done on vendors and service providers prior to signing or agreeing to contractual obligations.

NEVER	RARELY	SOMETIMES	USUALLY	ALWAYS WITHOUT EXCEPTION

In many cases it is necessary to include a "Please Explain" or "Please Provide Details" to interpret responses. A sample of a self-assessment questionnaire used by U.S. Customs Services is shown below to illustrate the challenges in designing questionnaires.

10.	The purpose of my (our) trip is or was: (Check one or both boxes, if applicable)	☐ Business	☐ Personal
11.	I am (We are) bringing fruits, plants, meats, food, soil, birds, snails, other live animals, wildlife products, farm products; or, have been on a farm or ranch outside the U.S.	☐ Yes	☐ No
12.	I am (We are) carrying currency or monetary instruments over $10,000 U.S., or foreign equivalent:	☐ Yes	☐ No
13.	I have (We have) commercial merchandise, U.S. or foreign: (Check one box only)	☐ Yes	☐ No
14.	The total value of all goods, including commercial merchandise, I/we purchased or acquired abroad and am/are bringing to the U.S. is:	▷	$_____ (U.S. Dollars)
(See the instructions on the back of this form under "Merchandise" and use the space provided there to list all the items you must declare. If you have nothing to declare, write "-0-" in the space provided above)			

STEP 4 Collect and summarize the information obtained. Assess the appropriateness of the design/format of the questions or statements used to obtain the responses. It is also useful to interview a sample of respondents for their views on the questionnaire format used.

STEP 5 Assess the need to quality assure/audit the reliability of the responses provided if done by work units/management. Historically, the reliability of responses provided to compliance self-assessment questionnaires has often been poor and drawing conclusions based on responses provided without independent validation of positive responses is often dangerous.

STEP 6 Regularly assess the value derived from the compliance assessment exercise versus the cost in terms of time and resources expended by both the group asking the questions and the units responding.

Focus on Risk - Compliance-Centric Approach

In a compliance-based approach the focus is generally on determining whether prescribed controls that the author of questionnaire has decided are "key" are in place. In a large percentage of situations the author(s) of the questionnaire have not clearly identified the end result objective(s) sought or attempted to identify and assess specific risks to the objective(s). A well designed compliance approach has an opportunity to include linked business objectives and risks as part of the explanation for each question so that people using the compliance questionnaire fully understand the importance of the control/procedure being queried. Unfortunately in practice this is rarely done.

PROCESS-CENTRIC APPROACH

STEP 1 This approach defines an organization in terms of business processes. Business processes can be further stratified in terms of core processes and supporting/service processes. This is the dominant approach in use today in many companies for SOX 404/NI 52-109 control effectiveness assessments.

An example for a company in the retail sector is noted below:

STRATEGIC MANAGEMENT PROCESSES - RETAIL CLIENT

Core Business Processes

Brand and Image Delivery
Product/Service Delivery
Customer Service Delivery

Resource Management Processes

Human Resource Management
Property Management
Regulatory Management
Financial/Treasury Management
Information/Management

Source: Auditing Organizations Through a Strategic System Lens - The KPMG Business Measurement Process , Bells, Marrs, Solomon, Thomas 1997

STEP 2 Having defined a business entity into a set of processes and sub processes, the objectives and sub objectives of each process and sub process should be identified and analyzed (i.e. the desired end results or outcomes). (NOTE: This step is often not given the attention it deserves)

STEP 3 Once specific objectives of the business processes are identified, the next step is to identify risks that threaten the process and sub process objectives, and document the controls currently used or in place to mitigate those risks. (NOTE: This step is also often not given the attention it deserves)

STEP 4 In cases where a process or sub process has prescribed controls that aren't being complied with, concerns are reported. In some cases the reliability of the risk descriptions must also be revisited. Although process error rates should be measured and tracked this step is not always given the attention it deserves.

STEP 5 Take steps to modify the control design to bring the business process into equilibrium (i.e. it is producing acceptable outcomes or results with an acceptable level of retained risk or has fully compliant controls), consider revising business objectives, or, as a last resort, consider exiting the business area or activity.

NOTE: In some instances companies represent that they are using a "process-centric" approach when they are, in fact, using a "compliance-centric" approach which has mandated specific controls. Testing primarily focuses on the existence/use of prescribed controls not true process analysis of the type envisioned in TQM.

Focus on Risk - Process-Centric Approach

How much attention is given to formally identifying and assessing risks to process objectives and/or processes in general is highly variable. The emphasis is rarely on identifying residual risk status or performance and frequently on identifying "control deficiencies".

OBJECTIVE-CENTRIC APPROACH

STEP 1 This approach begins by identifying one or more end result business objectives or statements of the desired outcomes or results necessary for a specific entity and/or sub unit to succeed or fulfill its business mandate. For companies using some variant of the "Balanced Scorecard Approach" these are sometimes referred to as Key Result Areas ("KRAs"). To meet emerging institutional investor expectations Risk Oversight Solutions believes that the process should focus on identifying top strategic/long term value creation objectives and top value preservation objectives. (objectives where non-achievement could materially negatively impact share value). A range of approaches exist to assist with this step. Some organizations already have clear statements of end result objectives as a result of use of "Balanced Scorecard" initiatives or result-focuses reward systems. The use of a corporate "OBJECTIVES REGISTER" with top value creation and preservation objectives is recommended. Risk Oversight Solutions offers a range of free tools to end users to implement objective centric ERM and internal audit available at http://riskoversightsolutions.com/ro-resources , including summary guidance how to populate an objectives register. More detailed training materials can be accessed by purchasing a QUICK START CAPABILITY TRANSFER package (see http://riskoversightsolutions.com/wp-content/uploads/2011/03/Features-and-Benefits-Overview-Risk-Oversight-Solutions.pdf for details) which includes a license to an extensive library of training and implementation aids and 15 hours of implementation advice.

STEP 2 Having identified a universe of end-result objectives the next step is to gather and/or consider available information to decide where detailed risk assessment is warranted given the cost, and the level of "RISK ASSESSMENT RIGOR" warranted. This can include information such as amount of information available on the current risk status, importance of the objective to the organization, importance of the objective to the work unit, the impact of non-achievement, current results being achieved, existence of insurance, and other factors. After completing this step specific business objectives are selected for additional formal assessment at an assigned level or RISK ASSESSMENT RIGOR. Prioritization of objectives is essential to ensure that the organization's investment in risk/control assessment time and effort will be worthwhile. In an ideal world, decisions on the amount or risk assessment rigor/formality are made by the owner/sponsor of the objective with oversight from senior management and the board of directors.

STEP 3 Having selected whole business units and/or specific objectives for review, they are then analyzed including identifying and assessing specific risks/threats to the achievement of the objective, identifying the "risk treatments" currently in place to mitigate the risks identified, and the residual risk situation or status that currently exists given the controls in use. The residual risk status can be further analyzed by subdividing the status information into "Concerns", "Indicator" data, "Impact" data, and "Impediment" information. Residual risk status information is designed to help decision makers make sound and defensible decisions on the acceptability or adequacy of the current risk treatment strategy and where to best allocate human and financial resources.

STEP 4 A decision is then made by the evaluator(s) of the acceptability of the residual risk status and overall level of certainty of achievement.

In cases where the residual risk status/certainty is considered unacceptable, three choices exist:

(a) Revise the risk treatment strategies to reduce the level or residual risk to one that is consistent with the organization's "risk appetite/tolerance".

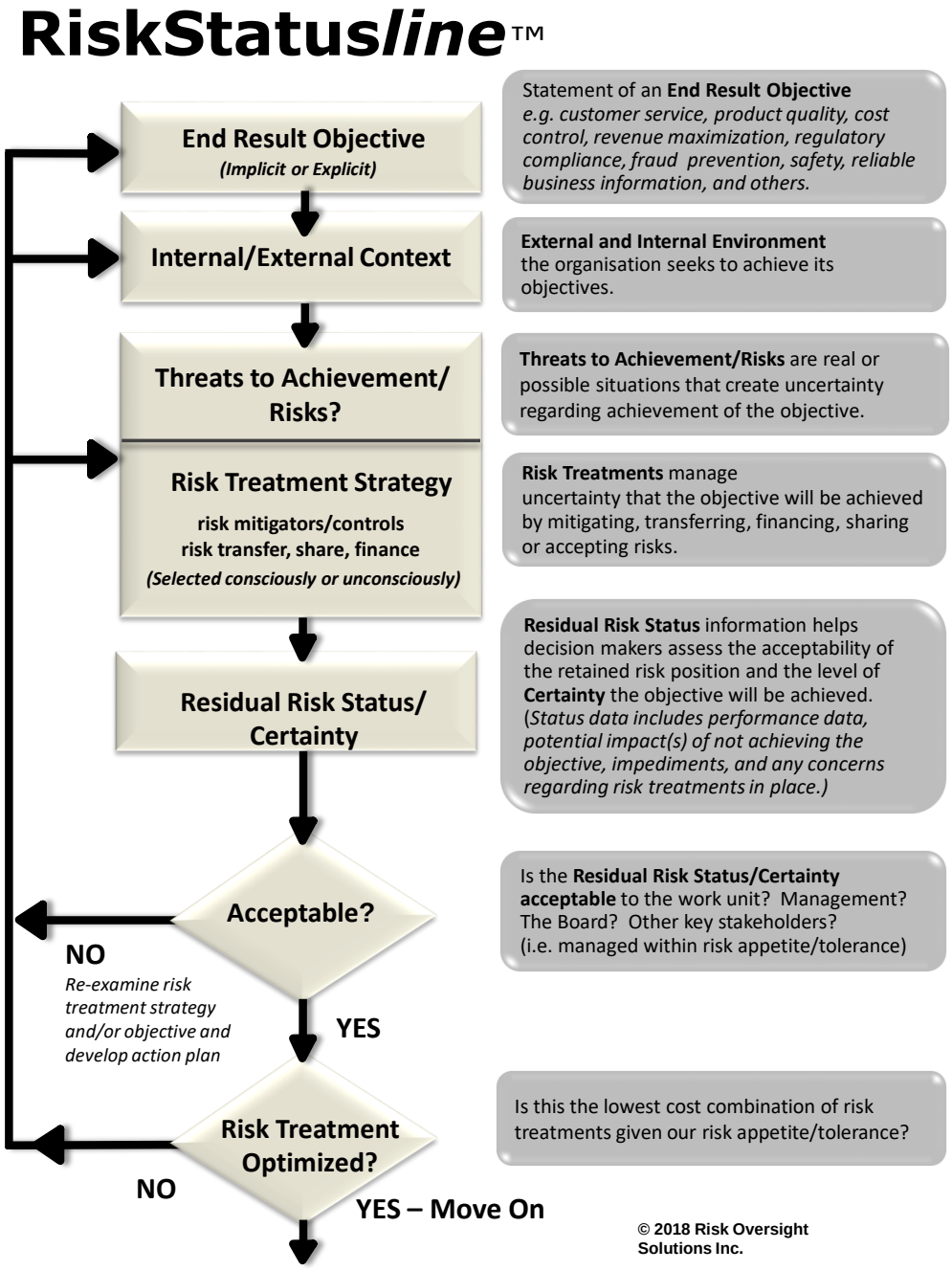
(b) Change the objective to bring the residual risk status in line with the objective.

(c) Discontinue the activity (i.e. avoid the risk)

Descriptions of some of the Risk Oversight Solutions implementation/training tools including the RiskStatus*line*™ diagram, Risk Sources model, Risk Design Principles and Risk Design elements are included on the pages that follow.

Focus on Risk - Objective-Centric Approach

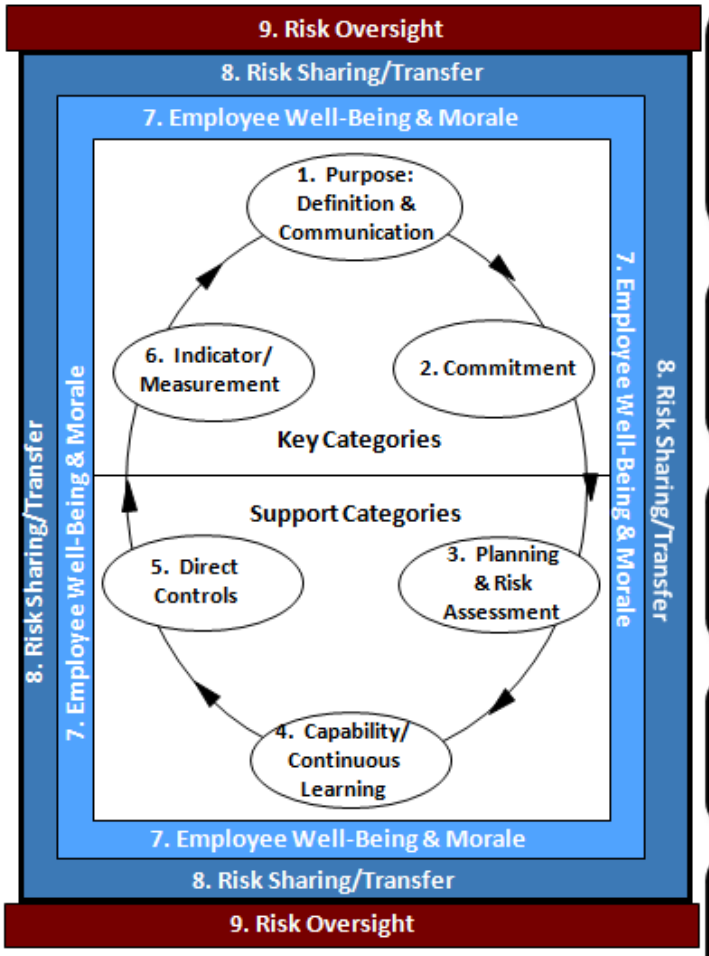
The focus in objective-centric approach is to identify a composite picture of the residual risk status linked to the objective. This includes information on the residual risk of individual risks as well as information on the current performance of the objective and impact to the organization of not achieving the objective in whole or in part.



RiskStatus*line*™
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?



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?

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

ro risk oversight solutions
A better response to risk.

Risk Oversight Solutions: Ten Primary Assurance Methods

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

RISK-CENTRIC APPROACH

STEP 1 Select the business entity, area or topic for assessment. (Sometimes referred to as the "context" of the risk assessment.)

STEP 2 Identify the risks or threats to the area or topic selected for review. Although many companies rely heavily on brainstorming and interviews to gather risks a range of techniques to complete this step exist including those listed below. More information on this step is included in Section 11.

(a) Consider all possible sources of risk. The Australian New Zealand standard on risk management utilizes 8 categories for this step - commercial and legal relationships, economic, human behaviour, natural events, political circumstances, technology, management activities and controls, individual activities. The Risk Oversight Solutions risk source framework has 16 risk source categories. Other, more detailed, risk source category systems exist that can be used to check the completeness of risks identified.

(b) Consider the different categories of business and quality objectives as a way of developing a list of risks. Examples of business objective categories include product quality, customer service, revenue generation, cost minimization, safety, reliability of business information, fraud prevention, asset safeguarding, continuity of operations, regulatory compliance, and internal compliance.

(c) Research known causes of failure or "loss events" to identify risks. The internet is now an excellent and cost effective way to identify sources of risk.

(d) Visualize plausible situations or circumstances related to the context being considered to identify potential risks. This should include a visual "walkthrough" of various plausible scenarios.

(e) Utilize the "inverse control model" approach. This technique relies on stating the inverse of a control category as a risk. Examples include:

i) Staff don't know who is responsible for the objective (Inverse of Risk Oversight's Risk Design Principles Category 1 - Purpose, Definition & Communication)
ii) Employees aren't committed to the issue (Inverse of Risk Oversight's Risk Design Principles Category 2)

STEP 3 Having enumerated a universe of risks or threats, these can then be ranked by considering their likelihood, consequences, and current "Risk Status".

This ranking process can be done using relatively simple rating methods, or employ sophisticated and complex numeric probability and sensitivity parameters and simulation techniques.

STEP 4 Specifically identify and document risk treatment elements/controls that mitigate or reduce the negative impacts of the risks selected for detailed examination. This can be done without a formal methodology or, alternatively, a risk treatment framework can be used to ensure that all relevant methods, procedures or other things that qualify as controls are considered and the root causes of problems identified. The use of a risk design model is strongly recommended. This step should also include identifying risk transfer/share/finance strategies or mechanisms.

STEP 5 Escalate upwards the risks which the assessors believe are not sufficiently mitigated or treated given the assessors' perception of the organization's tolerance for residual risk and risks which are significant enough to warrant special visibility and monitoring.

STEP 6 Periodically repeat the process and revisit the analysis and decisions in light of new information and/or circumstances.

NOTES:

"Risk Registers" are sometimes used to track risks identified and assign "risk owners". Risk registers may, or may not include a link to related business objectives. Risk "heat maps" are frequently used to display and report results. Most risk-centric approaches do not monitor the change in performance of objectives as a result of the use of formal assessment methods and/or changes in risk treatment design.

CONTROL-CENTRIC APPROACH

Control frameworks have been developed and used for various applications including criteria related to safety, product quality, customer service, financial statement reliability and many others. These frameworks implicitly, and in some cases explicitly, state that conformance to the criteria will result in positive or desired outcomes (e.g. reliable financial statements (COSO 2013 for SOX 404), environmental targets attained, high standards of product quality and customer service, etc.). Control models such as COSO 1992/2013, Cadbury, and CoCo are illustrations of such frameworks. Many other similar assessment criteria frameworks exist. Research to validate that conformance to the framework actually produces the positive results claimed by the authors of the framework is often not undertaken by the group that establishes the criteria/framework. (e.g. COSO Internal Control- Integrated Framework 2013)

STEP 1 Identify the business entity, sub entity, process or topic for assessment.

STEP 2 Select the control or quality model to be used. (e.g. COSO 2013, Risk Oversight Solutions Risk Treatment Principles, Criteria of Control ("CoCo"), Baldrige, customized framework, etc.

STEP 3 Obtain information on the level or extent that the area being reviewed uses, has in place, or otherwise manifests the specific elements or criteria in the model and list information on concerns and problems. This can be done subjectively by one or more specialist, using voting tools in group settings, or by rigorous data gathering and analysis by auditors.

STEP 4 Evaluate the information obtained. This may involve the use of interpretation guides provided by the model if any exist, or by subjective interpretations of the reviewer. (e.g. the Malcolm Baldrige quality system is a 1000 point. A score of 400 would suggest the ability of the organization to continually meet and exceed customer expectations is low relative to an entity that attains a score of 700 out of 1,000. Similarly a failure to satisfy or fulfill in a significant way various criteria defined in the COSO 2013 internal control framework would suggest deficiencies in the control environment which will reduce the probability of, or cause more variability in, the attainment of one or more organizational objectives.)

STEP 5 Having obtained information on the extent the area being evaluated manifests the various criteria in the framework, this information can then be visually depicted by way of bar graphs or other visual aids.

STEP 6 Periodically revisit the assumption that conformance to the criteria in the framework selected results in desired outcomes being achieved. If, for example, an organization strongly manifests all criteria of the COSO 2013 model, all things equal, the COSO 2013 authors imply that there is a higher likelihood of attaining its objectives, than there is in an organization that does not manifest the COSO 2013 criteria to the same extent. The validity of the model should be regularly revisited. Modifications should be made when the predictive ability of the model is weak (i.e. criteria or elements prescribed are present but desired results are not being achieved).

The 20 criteria in the now very dated by quite good Canadian Criteria of Control framework are shown on the next page. This framework suggests that organizations that demonstrate use of the 20 criteria have more assurance they will achieve their business objectives than those that don't demonstrate these attributes. Similar analysis can be done using other control frameworks like COSO 2013, quality, safety, environment and quality models. Automated tools can be effectively employed to improve the speed and reliability of the model criteria evaluation process.

CICA Guidance on Criteria of Control
The CoCo Criteria
November 1995

The CoCo Criteria	Description of Process in Place/Use	Subjective – Survey Based 0 = Not Evidenced 10 = Heavy Use/Evidence											Objective - Is Supported by Evidence 0 = Not Evidenced 10 = Heavy Use/Evidence											
PURPOSE			**0**										**10**		**0**										**10**
A1 Objectives should be established and communicated.		A1												A1											
A2 The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed.		A2												A2											
A3 Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated and practised so that people understand what is expected of them and the scope of their freedom to act.		A3												A3											
A4 Plans to guide efforts in achieving the organization's objectives should be established and communicated.		A4												A4											
A5 Objectives and related plans should include measurable performance targets and indicators.		A5												A5											
COMMITMENT																									
B1 Shared ethical values, including integrity, should be established, communicated and practised throughout the organization.		B1												B1											
B2 Human resource policies and practices should be consistent with an organization's ethical values and with the achievement of its objectives.		B2												B2											
B3 Authority, responsibility and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people.		B3												B3											
B4 An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives.		B4												B4											

Reprinted with permission from CICA Guidance on Control, The Canadian Institute of Chartered Accountants, Toronto, Canada.

CICA Guidance on Criteria of Control
The CoCo Criteria
November 1995

The CoCo Criteria	Description of Process in Place/Use	Subjective – Survey Based 0 = Not Evidenced 10 = Heavy Use/Evidence												Objective - Is Supported by Evidence 0 = Not Evidenced 10 = Heavy Use/Evidence											
CAPABILITY			**0**										**10**		**0**										**10**
C1 People should have the necessary knowledge, skills and tools to support the achievement of the organization's objectives.		C1												C1											
C2 Communication processes support the organization's values and the achievement of its objectives.		C2												C2											
C3 Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities.		C3												C3											
C4 The decisions and actions of different parts of the organization should be coordinated.		C4												C4											
C5 Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the inter-relatedness of control elements.		C5												C5											
MONITORING AND LEARNING																									
D1 External and internal environments should be monitored to obtain information that may signal a need to re-evaluate the organization's objectives or control.		D1												D1											
D2 Performance should be monitored against the targets and indicators identified in the organization's objectives and plans.		D2												D2											
D3 The assumptions behind an organization's objectives should be periodically challenged.		D3												D2											
D4 Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified.		D4												D4											
D5 Follow-up procedures should be established and performed to ensure appropriate change or action occurs.		D5												D5											
D6 Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable.		D6												D6											

Reprinted with permission from CICA Guidance on Control, The Canadian Institute of Chartered Accountants, Toronto, Canada

Understanding the 10 Main Assurance Strategies