



A better response to risk.

Objective Centric ERM & Internal Audit: Risk Culture Survey

Objective Centric ERM & Internal Audit can be implemented over time. Use our Risk Culture Survey to assess your next steps.

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

STEP 1 - SCORING YOUR RISK CULTURE

HISTORICAL/TRADITIONAL ASSURANCE	STEP 1: OBJECTIVELY SCORE YOUR ORGANIZATION'S CULTURE		SCORES	OBJECTIVE CENTRIC ERM AND INTERNAL AUDIT										
<ul style="list-style-type: none"> Assign Duties/Supervise Staff Policy/Rule Driven/Heavy use of intuitive risk management Risk/Assurance Data Developed and Stored in Silos Limited Employee ERM Participation and Training Narrow Stakeholder Focus Auditors and Other Specialists are the Primary Risk/Control Analysts/Reporters 	<p>1. SAFETY: Senior management encourages and rewards individuals and work units for analyzing and assessing risks to key value creation and preservation objectives and reporting risk status results upwards to the board --- even when the news is bad.</p> <p>0 1 2 3 4 5 6 7 8 9 10</p>		<p style="writing-mode: vertical-rl; transform: rotate(180deg);">SCORING 0 = STRONGLY DISAGREE 10 = STRONGLY AGREE</p>	<ul style="list-style-type: none"> C-Suite and Board have full responsibility for risk oversight and effectiveness of risk management processes Integration of the Efforts of All Assurance Participants Holistic, Anticipatory and Proactive Risk Assessments Are Linked to Objectives/Performance Info/Loss Events Consensus Agreement up to and including the board on Acceptable Residual Risk Status is a Primary Goal 										
<table border="0"> <thead> <tr> <th data-bbox="108 657 475 687">MANAGEMENT AND STAFF</th> <th data-bbox="475 657 826 687">AUDIT</th> </tr> </thead> <tbody> <tr> <td data-bbox="108 687 475 1755"> <ul style="list-style-type: none"> Often use intuitive and informal (versus formal) risk assessment methods. Receive limited formal training on risk assessment and risk treatment design. Often consider auditors, consultants, and other specialists to be the control experts. Outside specialists are sometimes hired to analyze and make recommendations in areas where concerns and/or problems exist. Are often not allowed or encouraged at lower levels to analyze and make decisions relating to risk acceptance or risk treatment strategies. The personnel doing the work are often not expected to identify, assess risks and select risk treatment strategies that help assure that objectives are achieved. Candid disclosure of the current state of residual risk status (areas of exposure) is not expected or encouraged, and is sometimes discouraged and punished. Fear and blame sometimes occur when problems surface. Internal control, risk management, total quality/continuous improvement are not integrated programs or concepts. </td> <td data-bbox="475 687 826 1755"> <ul style="list-style-type: none"> A primary objective is to perform audits and report on control effectiveness and control deficiencies to senior management, the board, and/or external stakeholders. Relations with audit clients are sometimes adversarial. Auditors are viewed as the control "experts". Risk and control assessment training is directed primarily to auditors and other specialists. A common audit objective is to report on whether units are complying with prescribed controls, procedures, and/or standards. How auditors decide what constitutes "effective" or "adequate" control, and how much risk is considered acceptable by them and why, is often not explicitly disclosed. Auditors are measured primarily on execution of prescribed audit processes. Auditors receive limited training on risk identification methods and measurement and ways to "optimize" risk treatment portfolios. (i.e. lowest cost possible to produce an acceptable level of residual risk) Internal auditors often focus on traditional financial areas and rarely report on risks to key strategic/value creation objectives. </td> </tr> </tbody> </table>	MANAGEMENT AND STAFF	AUDIT		<ul style="list-style-type: none"> Often use intuitive and informal (versus formal) risk assessment methods. Receive limited formal training on risk assessment and risk treatment design. Often consider auditors, consultants, and other specialists to be the control experts. Outside specialists are sometimes hired to analyze and make recommendations in areas where concerns and/or problems exist. Are often not allowed or encouraged at lower levels to analyze and make decisions relating to risk acceptance or risk treatment strategies. The personnel doing the work are often not expected to identify, assess risks and select risk treatment strategies that help assure that objectives are achieved. Candid disclosure of the current state of residual risk status (areas of exposure) is not expected or encouraged, and is sometimes discouraged and punished. Fear and blame sometimes occur when problems surface. Internal control, risk management, total quality/continuous improvement are not integrated programs or concepts. 	<ul style="list-style-type: none"> A primary objective is to perform audits and report on control effectiveness and control deficiencies to senior management, the board, and/or external stakeholders. Relations with audit clients are sometimes adversarial. Auditors are viewed as the control "experts". Risk and control assessment training is directed primarily to auditors and other specialists. A common audit objective is to report on whether units are complying with prescribed controls, procedures, and/or standards. How auditors decide what constitutes "effective" or "adequate" control, and how much risk is considered acceptable by them and why, is often not explicitly disclosed. Auditors are measured primarily on execution of prescribed audit processes. Auditors receive limited training on risk identification methods and measurement and ways to "optimize" risk treatment portfolios. (i.e. lowest cost possible to produce an acceptable level of residual risk) Internal auditors often focus on traditional financial areas and rarely report on risks to key strategic/value creation objectives. 	<p>2. TRUTHFULNESS/CANDOUR: Work unit members are comfortable discussing and dealing with tough issues including individual performance, business ethics, problems in their work unit, and high levels of retained risk.</p> <p>0 1 2 3 4 5 6 7 8 9 10</p>		<p style="writing-mode: vertical-rl; transform: rotate(180deg);">SCORING 0 = STRONGLY DISAGREE 10 = STRONGLY AGREE</p>	<table border="0"> <thead> <tr> <th data-bbox="2234 657 2582 687">MANAGEMENT AND STAFF</th> <th data-bbox="2582 657 2933 687">AUDIT</th> </tr> </thead> <tbody> <tr> <td data-bbox="2234 687 2582 1755"> <ul style="list-style-type: none"> Are accountable for designing and maintaining risk management systems that provide an acceptable level of residual risk to senior management and the board regarding the achievement of business objectives. Are provided with adequate risk assessment and design skills to fulfill their responsibility to report to senior management, the Board, and others on residual risk status. Consensus on relevant business objectives and levels of acceptable residual risk is a primary goal. Candid disclosure of the state of residual risk is encouraged and rewarded. Clear accountability for end result business objectives exists, and is accepted by staff at all levels, in all functions. Employees at all levels are responsible for finding new and better ways to improve and optimize risk treatment portfolios to better manage risk and achieve key business objectives while operating with an acceptable level of retained risk. Employees at all levels continually reassess the adequacy and appropriateness of risk treatment choices and make, or call for, adjustments when new information emerges regarding residual risk status, prioritization of objectives, and the risk treatment options available </td> <td data-bbox="2582 687 2933 1755"> <ul style="list-style-type: none"> Primary audit objectives are to: <ul style="list-style-type: none"> provide accurate and complete information to the Board, Senior Management and others on effectiveness of the entity's risk management processes and current state of residual risk status; raise risk assessment skills of all staff up to and including the Board; A key role is to foster more effective risk management through example, training, coaching, facilitation, and feedback - unless quality assurance reviews suggest that representations on risk status by work units and Owner/Sponsors are misleading and the "good faith" assumption is not appropriate. Auditors help ensure that the organization's business objectives are end-result focused and recognize a range of stakeholders, including customers and regulators; and objectives are aligned with the corporate mission/vision. Auditors are measured on, and accountable for, achievement of the primary objectives noted above, not completing spot-in-time audits and the annual audit plan. Auditors should be skilled risk analysts. These skills should extend to the full range of business objectives including share appreciation, revenue generation, customer service, product quality, compliance, fraud prevention and detection, safety, and environment as well as traditional financial/asset safeguarding objectives. </td> </tr> </tbody> </table>		MANAGEMENT AND STAFF	AUDIT	<ul style="list-style-type: none"> Are accountable for designing and maintaining risk management systems that provide an acceptable level of residual risk to senior management and the board regarding the achievement of business objectives. Are provided with adequate risk assessment and design skills to fulfill their responsibility to report to senior management, the Board, and others on residual risk status. Consensus on relevant business objectives and levels of acceptable residual risk is a primary goal. Candid disclosure of the state of residual risk is encouraged and rewarded. Clear accountability for end result business objectives exists, and is accepted by staff at all levels, in all functions. Employees at all levels are responsible for finding new and better ways to improve and optimize risk treatment portfolios to better manage risk and achieve key business objectives while operating with an acceptable level of retained risk. Employees at all levels continually reassess the adequacy and appropriateness of risk treatment choices and make, or call for, adjustments when new information emerges regarding residual risk status, prioritization of objectives, and the risk treatment options available 	<ul style="list-style-type: none"> Primary audit objectives are to: <ul style="list-style-type: none"> provide accurate and complete information to the Board, Senior Management and others on effectiveness of the entity's risk management processes and current state of residual risk status; raise risk assessment skills of all staff up to and including the Board; A key role is to foster more effective risk management through example, training, coaching, facilitation, and feedback - unless quality assurance reviews suggest that representations on risk status by work units and Owner/Sponsors are misleading and the "good faith" assumption is not appropriate. Auditors help ensure that the organization's business objectives are end-result focused and recognize a range of stakeholders, including customers and regulators; and objectives are aligned with the corporate mission/vision. Auditors are measured on, and accountable for, achievement of the primary objectives noted above, not completing spot-in-time audits and the annual audit plan. Auditors should be skilled risk analysts. These skills should extend to the full range of business objectives including share appreciation, revenue generation, customer service, product quality, compliance, fraud prevention and detection, safety, and environment as well as traditional financial/asset safeguarding objectives.
MANAGEMENT AND STAFF	AUDIT													
<ul style="list-style-type: none"> Often use intuitive and informal (versus formal) risk assessment methods. Receive limited formal training on risk assessment and risk treatment design. Often consider auditors, consultants, and other specialists to be the control experts. Outside specialists are sometimes hired to analyze and make recommendations in areas where concerns and/or problems exist. Are often not allowed or encouraged at lower levels to analyze and make decisions relating to risk acceptance or risk treatment strategies. The personnel doing the work are often not expected to identify, assess risks and select risk treatment strategies that help assure that objectives are achieved. Candid disclosure of the current state of residual risk status (areas of exposure) is not expected or encouraged, and is sometimes discouraged and punished. Fear and blame sometimes occur when problems surface. Internal control, risk management, total quality/continuous improvement are not integrated programs or concepts. 	<ul style="list-style-type: none"> A primary objective is to perform audits and report on control effectiveness and control deficiencies to senior management, the board, and/or external stakeholders. Relations with audit clients are sometimes adversarial. Auditors are viewed as the control "experts". Risk and control assessment training is directed primarily to auditors and other specialists. A common audit objective is to report on whether units are complying with prescribed controls, procedures, and/or standards. How auditors decide what constitutes "effective" or "adequate" control, and how much risk is considered acceptable by them and why, is often not explicitly disclosed. Auditors are measured primarily on execution of prescribed audit processes. Auditors receive limited training on risk identification methods and measurement and ways to "optimize" risk treatment portfolios. (i.e. lowest cost possible to produce an acceptable level of residual risk) Internal auditors often focus on traditional financial areas and rarely report on risks to key strategic/value creation objectives. 													
MANAGEMENT AND STAFF	AUDIT													
<ul style="list-style-type: none"> Are accountable for designing and maintaining risk management systems that provide an acceptable level of residual risk to senior management and the board regarding the achievement of business objectives. Are provided with adequate risk assessment and design skills to fulfill their responsibility to report to senior management, the Board, and others on residual risk status. Consensus on relevant business objectives and levels of acceptable residual risk is a primary goal. Candid disclosure of the state of residual risk is encouraged and rewarded. Clear accountability for end result business objectives exists, and is accepted by staff at all levels, in all functions. Employees at all levels are responsible for finding new and better ways to improve and optimize risk treatment portfolios to better manage risk and achieve key business objectives while operating with an acceptable level of retained risk. Employees at all levels continually reassess the adequacy and appropriateness of risk treatment choices and make, or call for, adjustments when new information emerges regarding residual risk status, prioritization of objectives, and the risk treatment options available 	<ul style="list-style-type: none"> Primary audit objectives are to: <ul style="list-style-type: none"> provide accurate and complete information to the Board, Senior Management and others on effectiveness of the entity's risk management processes and current state of residual risk status; raise risk assessment skills of all staff up to and including the Board; A key role is to foster more effective risk management through example, training, coaching, facilitation, and feedback - unless quality assurance reviews suggest that representations on risk status by work units and Owner/Sponsors are misleading and the "good faith" assumption is not appropriate. Auditors help ensure that the organization's business objectives are end-result focused and recognize a range of stakeholders, including customers and regulators; and objectives are aligned with the corporate mission/vision. Auditors are measured on, and accountable for, achievement of the primary objectives noted above, not completing spot-in-time audits and the annual audit plan. Auditors should be skilled risk analysts. These skills should extend to the full range of business objectives including share appreciation, revenue generation, customer service, product quality, compliance, fraud prevention and detection, safety, and environment as well as traditional financial/asset safeguarding objectives. 													
<p>3. EMPOWERMENT: Decisions are made to the extent possible by people in the best position to make the decision, not based on positional status or precedent.</p> <p>0 1 2 3 4 5 6 7 8 9 10</p>		<p style="writing-mode: vertical-rl; transform: rotate(180deg);">SCORING 0 = STRONGLY DISAGREE 10 = STRONGLY AGREE</p>												
<p>4. TRAINING: People at all levels regularly take training to increase their knowledge and skills in areas related to the successful achievement of business objectives and risk management.</p> <p>0 1 2 3 4 5 6 7 8 9 10</p>			<p style="writing-mode: vertical-rl; transform: rotate(180deg);">SCORING 0 = STRONGLY DISAGREE 10 = STRONGLY AGREE</p>											
<p>5. CREATIVITY/INNOVATION: People at all levels are encouraged to be creative and innovative in the quest for continuous improvement of risk treatment designs.</p> <p>0 1 2 3 4 5 6 7 8 9 10</p>				<p style="writing-mode: vertical-rl; transform: rotate(180deg);">SCORING 0 = STRONGLY DISAGREE 10 = STRONGLY AGREE</p>										
<p>6. RIGOUR: Work units regularly examine and assess their work processes and continually seek new and better ways to manage risks to key objectives.</p> <p>0 1 2 3 4 5 6 7 8 9 10</p>					<p style="writing-mode: vertical-rl; transform: rotate(180deg);">SCORING 0 = STRONGLY DISAGREE 10 = STRONGLY AGREE</p>									
<p style="text-align: right;">TOTAL SCORE</p>						<p style="writing-mode: vertical-rl; transform: rotate(180deg);">SCORING 0 = STRONGLY DISAGREE 10 = STRONGLY AGREE</p>								

STEP 2: SELECT AN APPROPRIATE IMPLEMENTATION OPTION

Strong Attachment and Preference For the Historical/Traditional Approach (Score 0-25)

- Provide training to management personnel, assurance specialists, and auditors on risk assessment and risk treatment design.
- Provide people involved in developing and writing corporate policies with training on defining end result objectives and risk assessment and risk treatment design.
- If risk self-assessment is done by work units at all carefully assess the cultural fit, particularly organization receptivity/safety linked to candid disclosure of serious risk exposures/problems.
- When completing audits the auditors document and rank key end-result objectives, identify and assess risks and related risk treatment strategies, document the current residual risk status, and offer recommendations. Whether it is the auditors or management personnel that decide on the acceptability of current residual risk status is variable.
- Provide briefings/training to senior management and the Board on emerging board risk oversight expectations and tools.

Middle Ground - Shifting the Culture (Score 26-40)

- Limited and very careful use of work unit risk self-assessment process and tools.
- Offer risk self-assessment services to work units or divisions that are receptive and appear to be reasonably "safe" (i.e. people in the area can talk about problems without fear).
- Offer risk assessment and risk treatment design training to any work units or managers that are interested.
- Continue to sell senior management and the Board on the tangible benefits available from fully integrated ERM, including benefits that can accrue from enhanced risk oversight in the eyes of credit rating agencies, institutional investors, securities regulators, other regulators, and other key stakeholders.
- Require that business units and senior executives provide regular representations to the Board on areas of significant retained/residual risk. These should be supported by demonstrable evidence and be auditable.
- If the board and senior management are supportive of shifting the culture, implement some form of formal risk self-assessment across the whole organization. Be alert for major resistance to change and "shoot the messenger" instances.

Integrated ERM is A Way of Life (Score 41-60)

- Fully implement "Objective Centric ERM and Internal Audit".
- Business objectives "Owner/Sponsors" make first level decisions on the level or risk assessment rigor on the objectives assigned. Risk assessment rigor decisions are reviewed and agreed by a senior management "Risk Oversight Committee". Owner/Sponsors regularly report "Composite Residual Risk Ratings" ("CRRR) upwards to senior management and the Board.
- Owner/Sponsors and other key staff receive training on risk assessment and risk treatment methods and tools.
- ERM specialists, internal auditors and other assurance specialists provide risk management training, coaching and quality assurance services.
- Owner/Sponsors decide on other staff that would benefit from risk assessment skills training.
- Management-by-fact, including candid disclosure of the current residual risk status, is an obsession that is fostered, recognized and rewarded.
- The Officers and the Board provide genuine tangible support and encouragement for integrated enterprise risk management and candid reporting on residual risk status.
- Feedback is provided to Owner/Sponsors on the quality of their risk self-assessments by Internal Audit or other independent assurance staff to help them improve their risk assessment and risk treatment design skills.