RISK OVERSIGHT
SOLUTIONS

Using Objective Centric Risk Assessment for SOX 404 and SOX 404 like requirements

Tim Leech, Managing Director
Risk Oversight Solutions Inc.
timleech@riskoversightsolutions.com

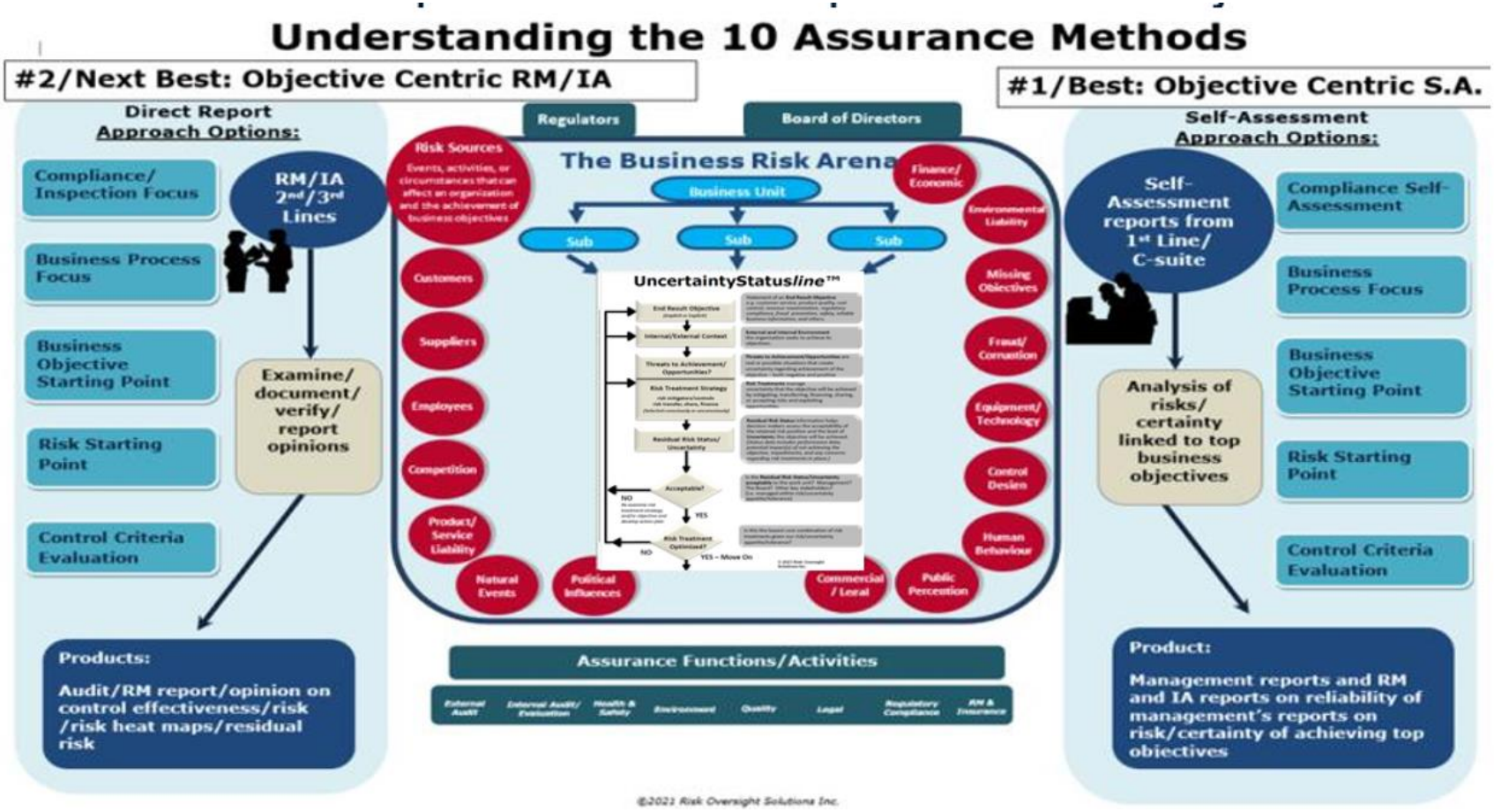
www.riskoversightsolutions.com

Module Coverage

Using Objective Centric Risk Assessment for SOX 404 and similar national requirements

- Understanding 5 primary assurance methods
- Completing macro level reliable financial statements assessments – key concepts
- Completing Line item/sub-objective assessments
- Reporting results to CEO/CFO/Board
- Benefits of using objective centric assurance for financial statements reporting

Understanding the 5 Primary Assurance Methods



RISK OVERSIGHT SOLUTIONS

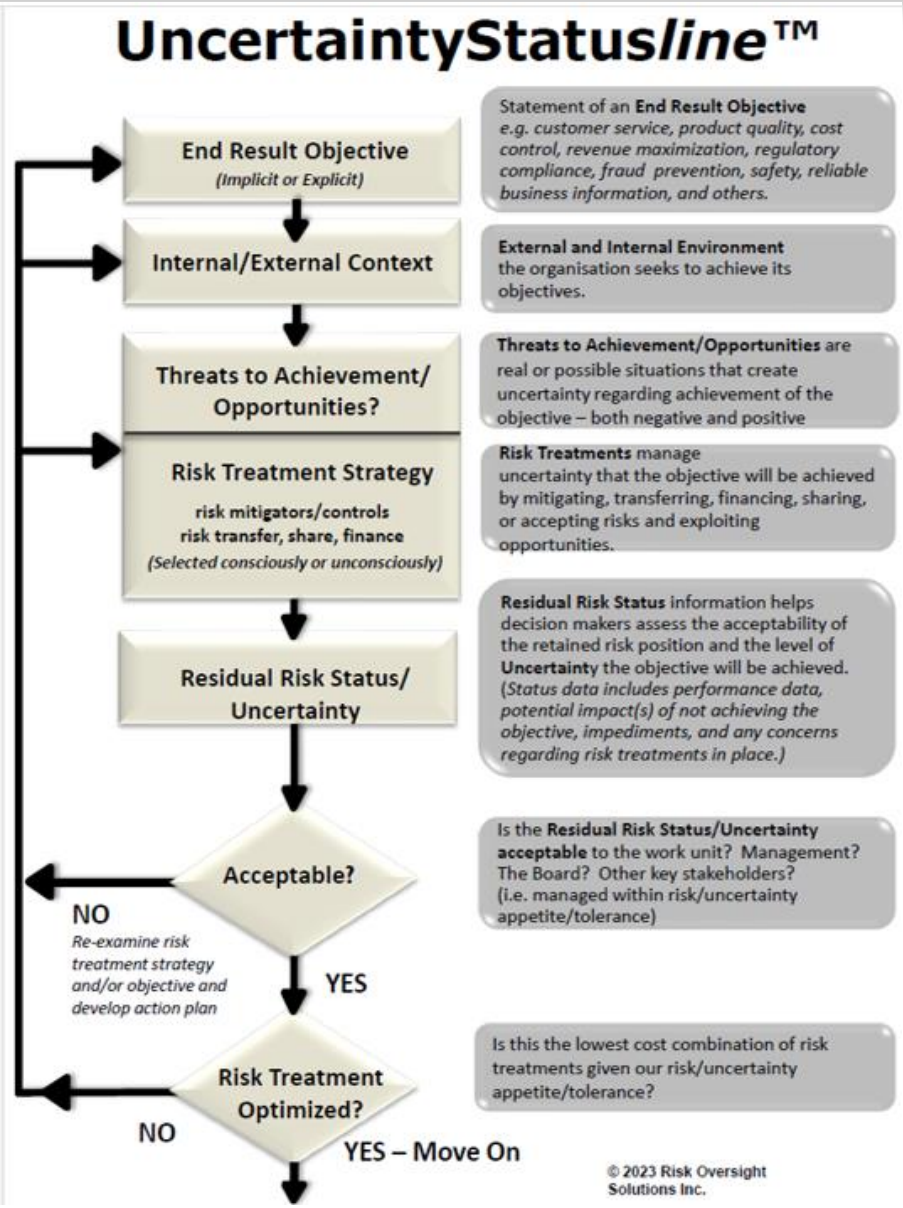
Macro Level Risk Assessments

Macro Objective:

Ensure ABC's financial statements are materially reliable in accordance with applicable GAAP and, in the U.S., "internal controls" are "effective" in accordance with a "suitable" internal control framework, usually COSO ICIF 2013.

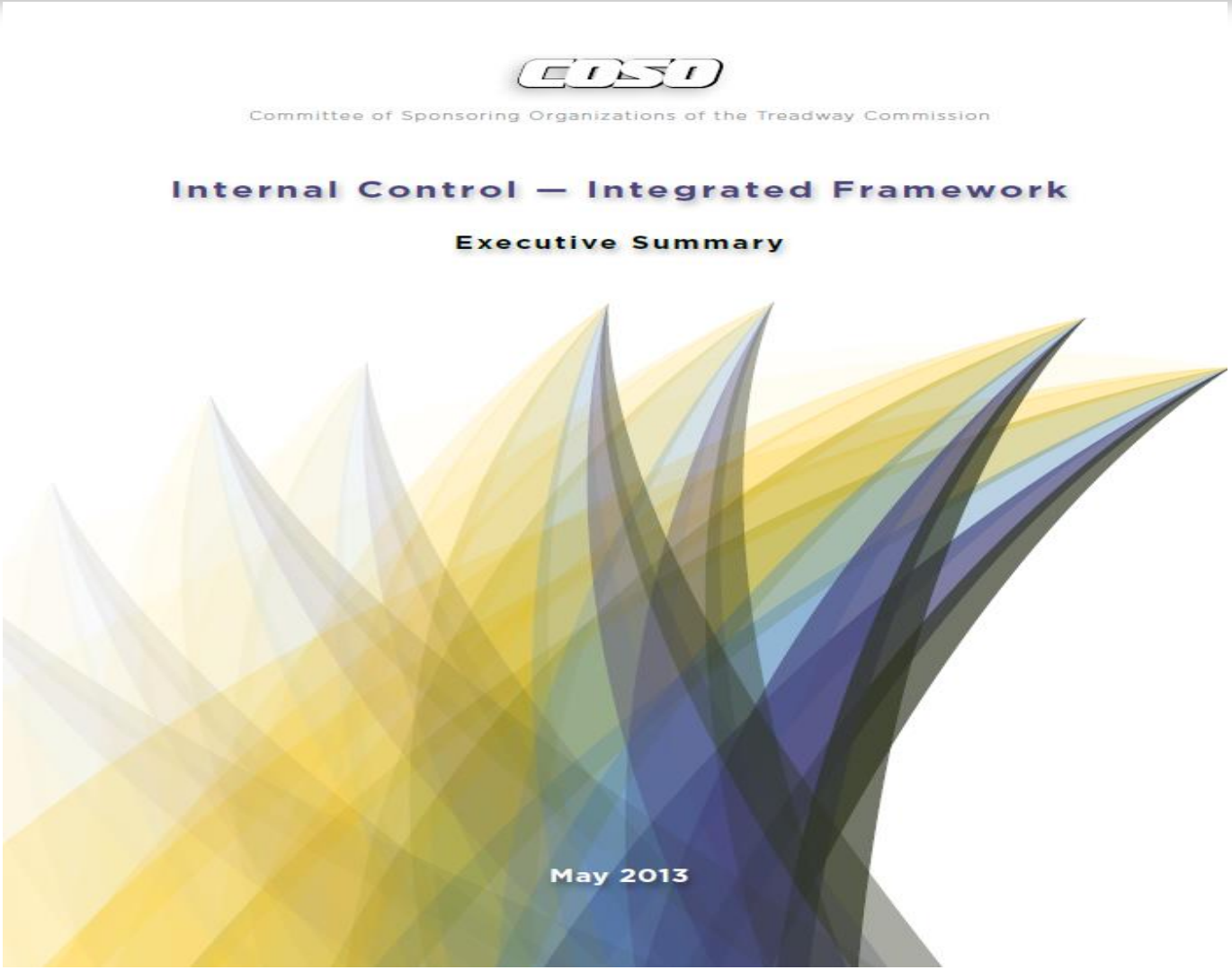
We strongly recommend that a macro risk assessment be done first; and then decisions made on the need for separate more detailed assessments of supporting sub-objectives including important note and supplemental disclosures.

Macro Level Risk Assessments



RISK OVERSIGHT SOLUTIONS

Macro Level Risk Assessments



Macro Level Risk Assessment

RISK OVERSIGHT SOLUTIONS

Macro Level Risk Assessment

Research done by Institute of Management Accountants issued in 2006 4 years post SOX indicated not many companies could demonstrate with clarity how their financial reporting internal controls are, or are not, “effective” in accordance with the COSO Internal Control Integrated Framework

Macro Level Risk Assessment

RISK OVERSIGHT SOLUTIONS

Macro Level Risk Assessment

TABLE 15. DID THE SOX COMPLIANCE TEAM IDENTIFY PLAUSIBLE RISKS?

Question Statement	Extent to which Plausible Risks Identified (N=372)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. For the majority of your *financial statement accounts*, to what extent did your SOX 302/404 compliance team identify the plausible risks that could threaten the integrity of the balance in each one of the accounts?	4.6% (17)	20.7% (77)	25.0% (93)	47.3% (176)	2.4% (9)
2. For the majority of your *financial statement note disclosures*, to what extent did your SOX 302/404 compliance team identify the plausible risks that could threaten the integrity of the information in each one of the note disclosures?	8.3% (31)	29.0% (108)	26.3% (98)	30.1% (112)	6.25% (23)
3. To what extent did your SOX 302/404 compliance team identify plausible *IT-related* risks (e.g., infrastructure, access, integrity, security, etc.) for each application that impacts financial statement accounts and note disclosures?	1.6% (6)	18.0% (67)	25.0% (93)	53.5% (199)	1.9% (7)

Macro Level Risk Assessment

TABLE 16. USE OF THE COSO 1992 FRAMEWORK PRIOR TO SOX BY COMPANY MANAGEMENT

Response Scale	Q1: Extent to which COSO 1992 was utilized by our company to manage its enterprise risk and controls		
	Overall Sample (N=373)	Internal Auditors (N=146)	Management-types (N=227)
	% of Total	% of Total	% of Total
1. No Extent	37.8% (141)	45.9% (67)	32.6% (74)
2. Some Extent	31.4% (117)	30.1% (44)	32.2% (73)
3. Moderate Extent	13.9% (52)	11.6% (17)	15.4% (35)
4. Large Extent	11.3% (42)	7.5% (11)	13.7% (31)
5. Not Sure	5.6% (21)	4.8% (7)	6.2% (14)

Macro Level Risk Assessment

TABLE 17. USE OF THE COSO 1992 FRAMEWORK PRIOR TO SOX BY EXTERNAL AUDITORS

Response Scale	Q2: Extent to which COSO 1992 was utilized by your external auditors to size up the effectiveness of your system of internal control and share this assessment annually with the company management		
	Overall Sample (N=373)	Internal Auditors (N=146)	Management-types (N=227)
	% of Total	% of Total	% of Total
1. No Extent	23.6% (88)	30.1% (44)	19.4% (44)
2. Some Extent	29.5% (110)	28.8% (42)	30.0% (68)
3. Moderate Extent	13.9% (52)	11.6% (17)	15.4% (35)
4. Large Extent	7.2% (27)	5.5% (8)	8.4% (19)
5. Not Sure	25.7% (96)	24.0% (35)	26.9% (61)

Macro Level Risk Assessment

TABLE 20. PERCEPTIONS ABOUT COSO 1992 MEETING THE SEC CRITERIA OF SUITABILITY

Criteria for an Acceptable Control Evaluation Framework per Section 404 Final Rules	Extent to which COSO 1992 meets each one of the four criteria (N=301)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. Is free from bias	2% (7)	23% (68)	28% (85)	36% (108)	11% (33)
2. Permits reasonably consistent qualitative and quantitative measurements of a company's internal control over financial reporting	5% (15)	25% (74)	28% (85)	34% (102)	8% (25)
3. Is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal control over financial reporting are not omitted	3% (8)	25% (75)	27% (82)	36% (108)	9% (28)
4. Is relevant to an evaluation of internal control over financial reporting	2% (6)	22% (65)	27% (82)	40% (121)	9% (27)

Note: Percentages are rounded.

RISK OVERSIGHT SOLUTIONS

Macro Level Risk Assessment

TABLE 23. IS IT POSSIBLE TO ARRIVE AT A RELIABLE PASS/FAIL CONCLUSION ON ICOFR USING COSO 1992?

Response Scale	# of Respondents (N=327)	% of the Total Sample	Small Companies (N=62)	Medium to Large Companies (N=265)
1. No Extent	8	2.4%	0.0%	3.0%
2. Some Extent	163	49.8%	58.1%	47.9%
3. Moderate Extent	59	18.0%	16.1%	18.5%
4. Large Extent	72	22.0%	16.1%	23.4%
5. Uncertain	25	7.6%	9.7%	7.2%

TABLE 24. CONSENSUS IN CONCLUSIONS BETWEEN MANAGEMENT AND EXTERNAL AUDITOR USING COSO 1992

Response Scale	# of Respondents (N=327)	% of the Total Sample	Small Companies (N=62)	Medium to Large Companies (N=265)
1. No Extent	10	3.1%	1.6%	3.4%
2. Some Extent	166	50.8%	58.1%	49.1%
3. Moderate Extent	61	18.7%	19.4%	18.5%
4. Large Extent	58	17.7%	12.9%	18.9%
5. Uncertain	32	9.8%	8.1%	10.2%

Macro Level Risk Assessment

TABLE 27. RELIANCE ON FIVE COSO 1992 COMPONENTS TO EVALUATE CONTROLS FOR SPECIFIC ACCOUNT BALANCES

Five Components of the COSO 1992 Framework	Extent to which your SOX Compliance Team Relied on Five COSO Components while Evaluating Internal Controls over Specific Account Balances (N=327)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. Control Environment	6% (20)	28% (91)	31% (102)	31% (102)	4% (12)
2. Risk Assessment	7% (23)	32% (106)	34% (111)	23% (75)	4% (12)
3. Control Activities	4% (12)	23% (75)	30% (99)	39% (129)	4% (12)
4. Information and Communication	7% (23)	36% (119)	28% (93)	23% (74)	6% (18)
5. Monitoring	6% (21)	31% (101)	31% (102)	27% (89)	4% (14)

Note: Percentages are rounded.

RISK OVERSIGHT SOLUTIONS

Macro Level Assessment

Per COSO page 8 Executive Summary

“an effective system provides reasonable assurance regarding achievement of an entity’s objectives.”

“reasonable assurance” = acceptable uncertainty

Objective Centric Risk and Certainty Management and UncertaintyStatusline have been designed to allow a fact-based determination of what’s reasonable assurance/acceptable uncertainty. UncertaintyStatusline Risk Treatment Principles and sub-elements map directly to COSO 2013 ICFR

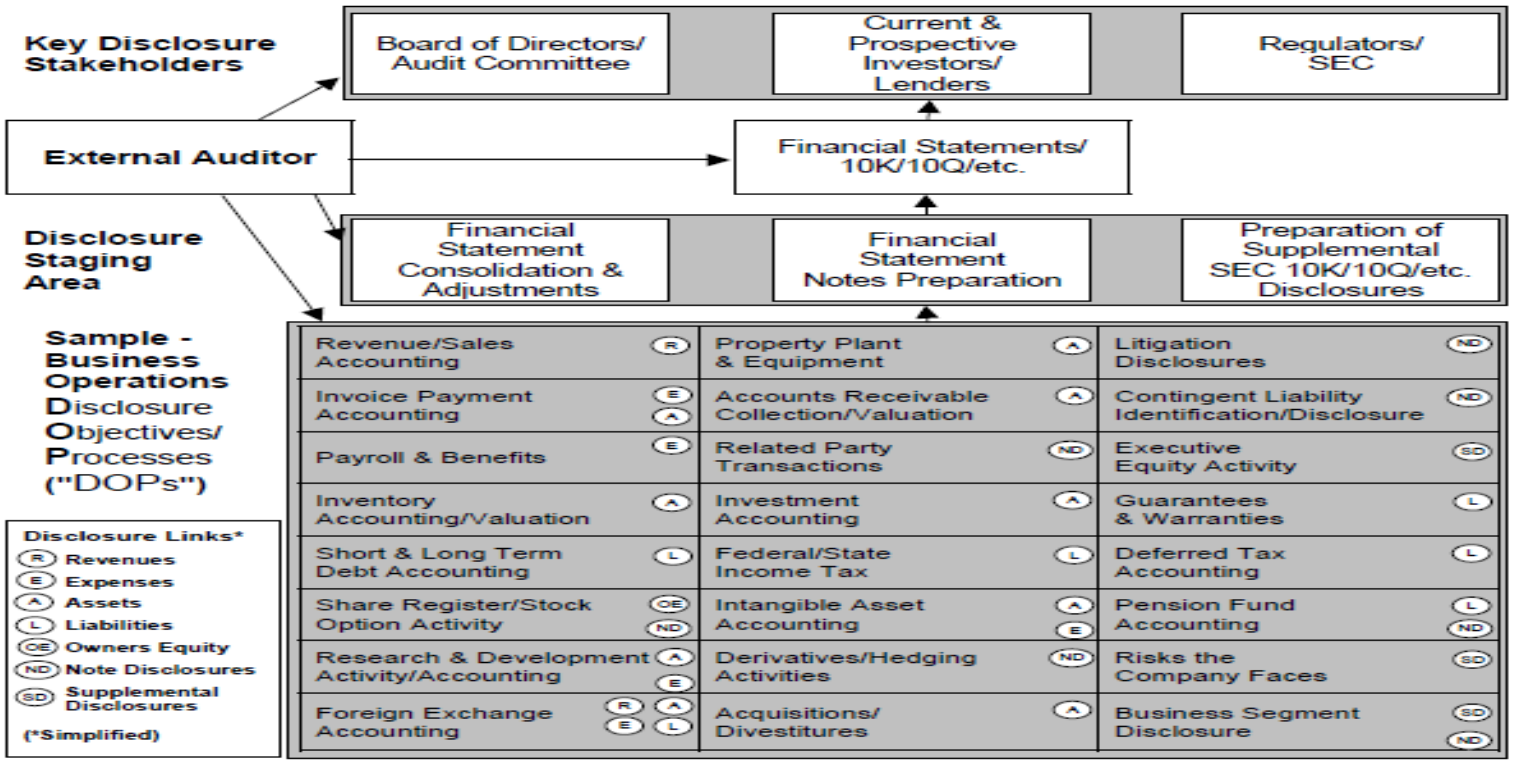
Macro Level Assessment

VISUALIZING THE GOALS OF SECTIONS 302 and 404

The fundamentals of sections 302 and 404 can be explained using the diagram below. The primary goal of the disclosure system is summarized in the purpose statement of SarbOx:

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws, and for other purposes.

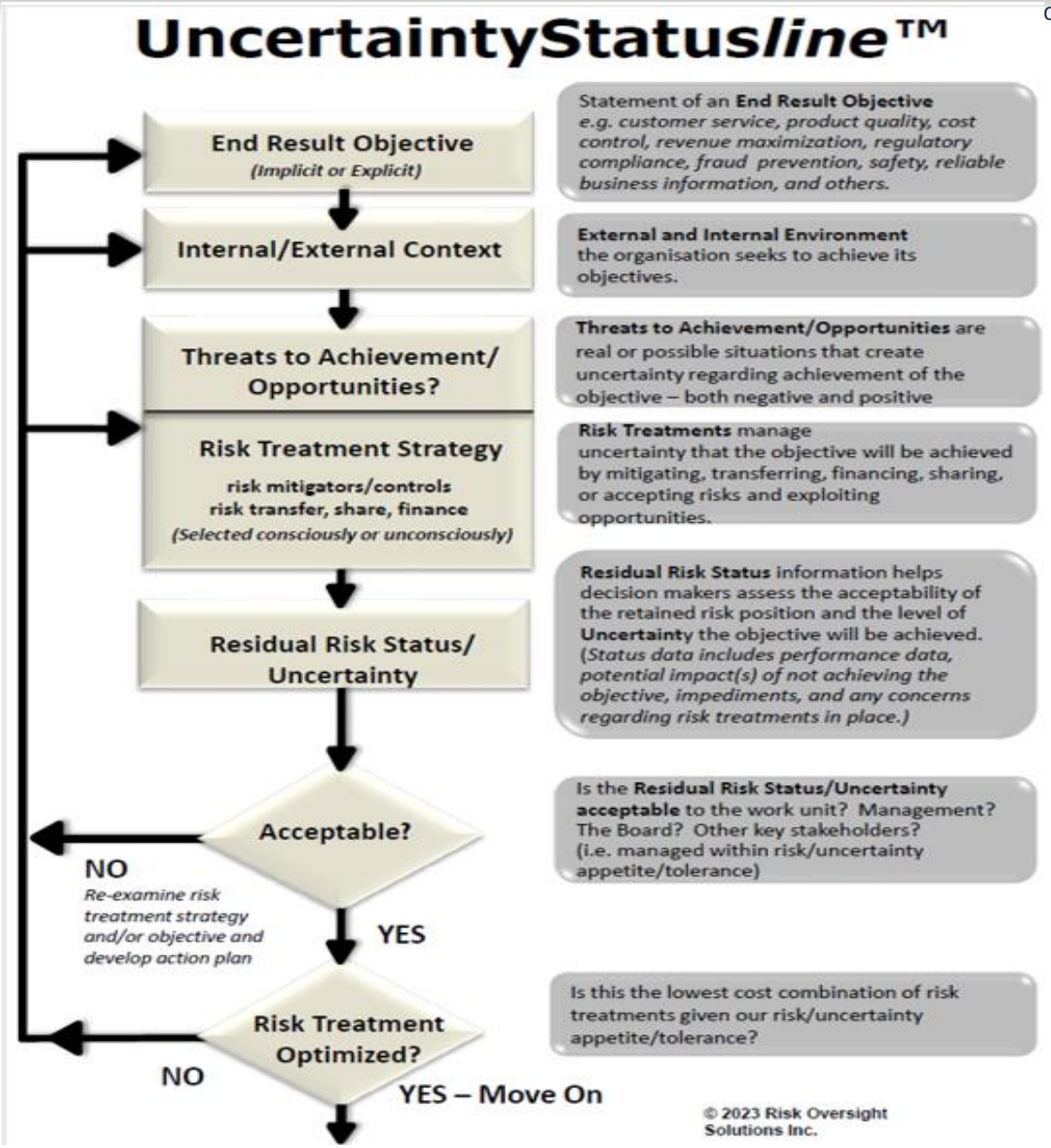
Sarbanes-Oxley
Section 302 & 404 Overview



RISK OVERSIGHT SOLUTIONS

Macro Level Assessment: Step by Step

Oversight Solutions Inc.



RISK OVERSIGHT SOLUTIONS

Macro Level Assessment: Step by Step

Internal/External Context

- Implications to the company's credit rating
- Implications to the company's reputation
- Implications to the company's cost of capital
- Personal implications to senior executives and board members
- Audit firm resignations/refusals
- Impact on the company's share price
- Personal philosophy of the company's CEO, CFO and Board of Directors
- Likelihood External Auditor Opinion on Financial Statements is wrong

Macro Level Assessment: Step by Step

Internal/External Context

- 1. Detected error history – external auditor
- 2. Detected error history – management detected after release of statements
- 3. Detected error history – management detected prior to release of statements
- 4. Complexity of accounting
- 5. Absolute dollar/unit of local currency value/impact of location/account
- 6. Detected error history – regulators/tax authorities/customers/others
- 7. Detected error history – internal audit
- 8. Detected/known errors in other companies in the same business sector
- 9. Amount of management judgment/subjectivity
- 10. Importance of account/location to security analysts
- 11. Importance of account/note disclosure to debt covenants
- 12. Susceptibility of account to fraud from insiders
- 13.Susceptibility of account to fraud from outsiders
- 14. Account/note linkage to the company's reward/compensation system

Macro Level Assessment: Step by Step

IDENTIFYING RISKS/THREATS TO ACHIEVEMENT

NOTE: refer to OCRUM learning module on identifying risks for information on the full range of risk identification methods available

1. **Research/AI and observation**
2. **Company Specific History**
3. **Experience of senior level staff**
4. **Industry specific scenario analysis**
5. **Risk source analysis**
6. **Industry "CHECK LISTS"**

Macro Level Assessment: Step by Step

IDENTIFYING RISKS/THREATS TO ACHIEVEMENT

Some statistically predictable risk examples. Ask Chat GPT for statistically significant risks.

1. CEO and CFO have significant financial incentives to falsify and/or inappropriately manage financial results.

2. Senior management has major financial incentives to direct backdating of stock options.

3. Senior management directs improper/fraudulent post-close journal entries to manage profits and/or hit earning targets disclosed to the market.

4. Management overrides controls to hit bonus targets or prevent loss of positions.

5. Audit Committees have financial incentives not to ask management tough questions.

Macro Level Assessment: Step by Step

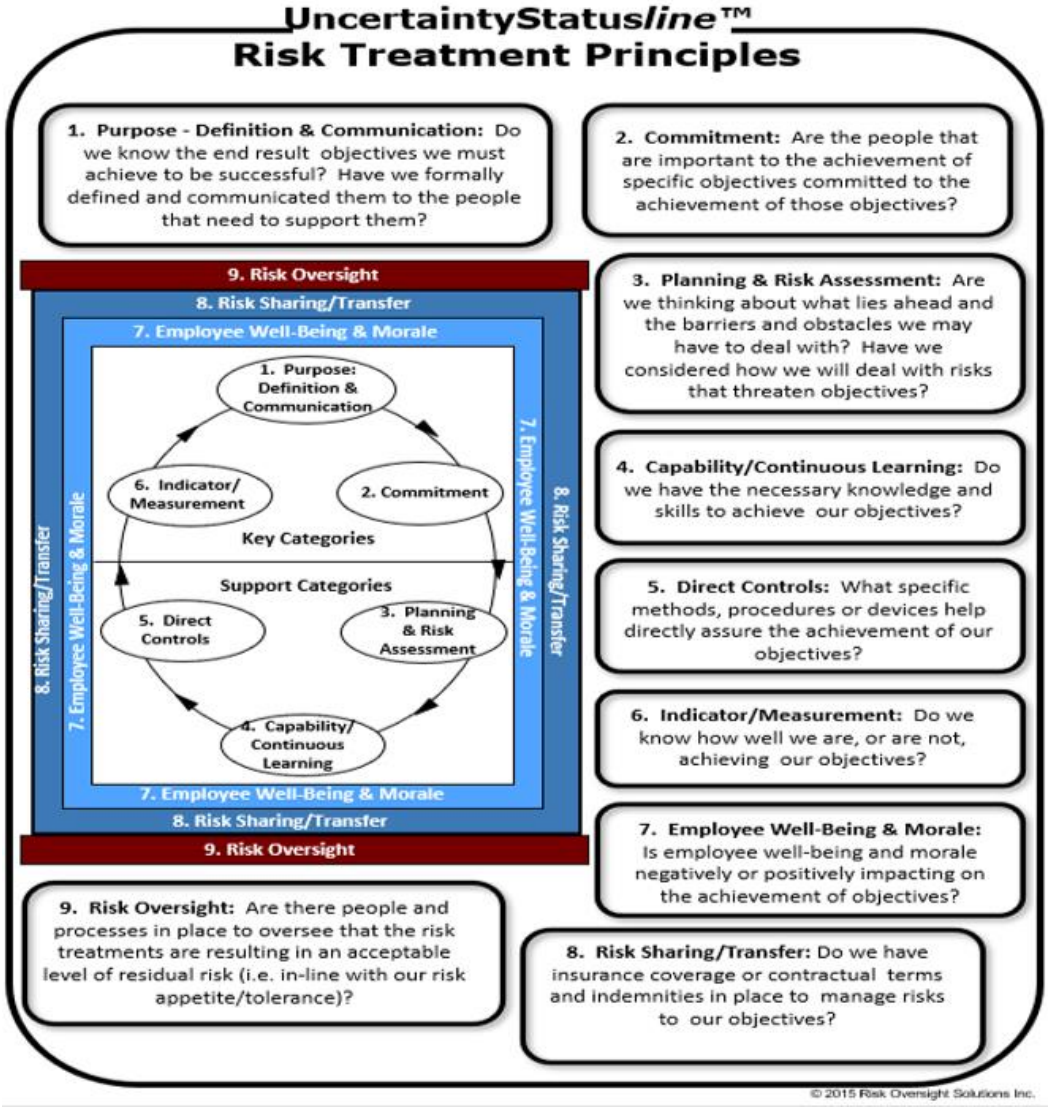
IDENTIFYING RISKS/THREATS TO ACHIEVEMENT

Some statistically predictable risk examples continued

6. Accounting staff are not current on accounting standards.
7. Management lacks the appropriate knowledge and skills to deal with accounting for complex or significant judgement related transactions.
8. In-house accounting personnel lack the necessary training and experience to deal with the scope of the organization's operations.
9. The external audit team's objectivity is compromised by conflicts of interest.
10. External audit team lacks appropriate knowledge/skills, and/or the courage to challenge management's assumptions.

Macro Level Assessment: Step by Step

IDENTIFYING RISKS TREATMENTS



RISK OVERSIGHT SOLUTIONS

Macro Level Assessment: Step by Step

IDENTIFYING RISKS TREATMENTS

Risk Treatment Principles 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

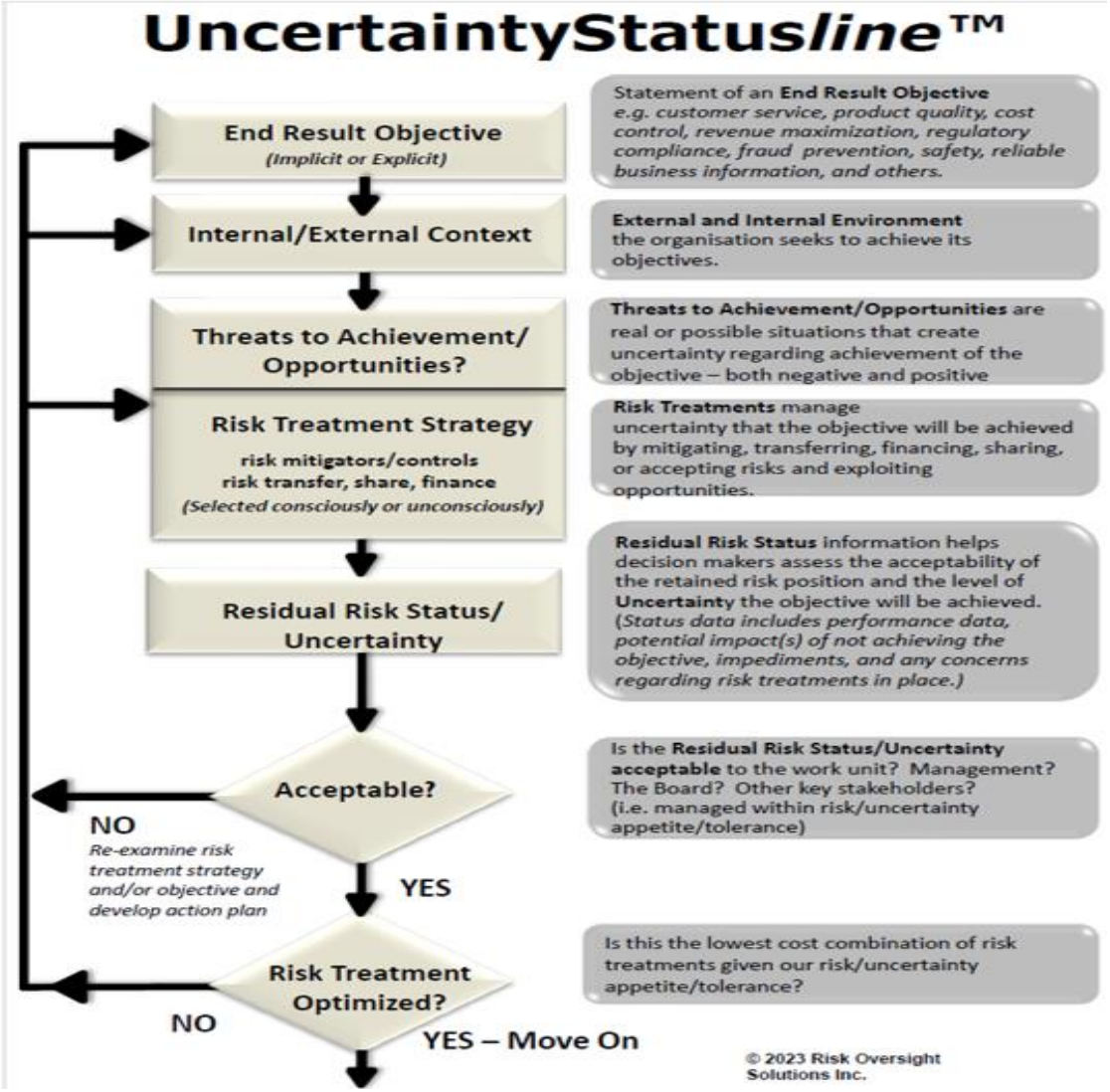
7. EMPLOYEE WELL-BEING & MORALE
- 7.1 Employee Surveys
- 7.2 Employee Focus Groups
- 7.3 Employee Question/Answer Vehicles
- 7.4 Management Communication Processes
- 7.5 Personal and Career Planning
- 7.6 Diversity Training/Recognition
- 7.7 Equity Analysis Processes
- 7.8 Measurement Tools/Processes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

Macro Level Assessment: Step by Step

IDENTIFYING RESIDUAL RISK STATUS/UNCERTAINTY



RISK OVERSIGHT SOLUTIONS

Real Life Risk Examples

- **Threat to Achievement/Risk Description:** Events, activities, current/known developments and contracts outside of the accounting department are not known and may affect financial statements.

Real Life Risk Examples

- **Threat to Achievement/Risk Description:** Time constraints during close related to journal entry preparation and check, as well as reporting/analysis may cause human errors to go undetected.

Real Life Risk Examples

- **Threat to Achievement/Risk Description:** Manual inputs from accounting personnel in the system are incorrect because of time constraints, volume/complexity of formulas, knowledge deficiencies (e.g. chemical usage, unbilled revenue).

Completing Sub-Objectives

VISUALIZING THE GOALS OF SECTIONS 302 and 404

The fundamentals of sections 302 and 404 can be explained using the diagram below. The primary goal of the disclosure system is summarized in the purpose statement of SarbOx:

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws, and for other purposes.

Sarbanes-Oxley
Section 302 & 404 Overview

Key Disclosure Stakeholders

Board of Directors/ Audit Committee | Current & Prospective Investors/ Lenders | Regulators/ SEC

External Auditor → Financial Statements/ 10K/10Q/etc.

Disclosure Staging Area

Financial Statement Consolidation & Adjustments | Financial Statement Notes Preparation | Preparation of Supplemental SEC 10K/10Q/etc. Disclosures

Sample - Business Operations Disclosure Objectives/ Processes ("DOPs")

Revenue/Sales Accounting (R)	Property Plant & Equipment (A)	Litigation Disclosures (ND)
Invoice Payment Accounting (E) (A)	Accounts Receivable Collection/Valuation (A)	Contingent Liability Identification/Disclosure (ND)
Payroll & Benefits (E)	Related Party Transactions (ND)	Executive Equity Activity (SD)
Inventory Accounting/Valuation (A)	Investment Accounting (A)	Guarantees & Warranties (L)
Short & Long Term Debt Accounting (L)	Federal/State Income Tax (L)	Deferred Tax Accounting (L)
Share Register/Stock Option Activity (OE) (ND)	Intangible Asset Accounting (A) (E)	Pension Fund Accounting (L) (ND)
Research & Development Activity/Accounting (A) (E)	Derivatives/Hedging Activities (ND)	Risks the Company Faces (SD)
Foreign Exchange Accounting (R) (A) (E) (L)	Acquisitions/ Divestitures (A)	Business Segment Disclosure (SD) (ND)

Disclosure Links*
- (R) Revenues
- (E) Expenses
- (A) Assets
- (L) Liabilities
- (OE) Owners Equity
- (ND) Note Disclosures
- (SD) Supplemental Disclosures

(*Simplified)

Completing Sub-Objectives

Deciding which disclosure line items warrant detailed risk assessment

- 1. Detected error history – external auditor
- 2. Detected error history – management detected after release of statements
- 3. Detected error history – management detected prior to release of statements
- 4. Complexity of accounting
- 5. Absolute dollar/unit of local currency value/impact of location/account
- 6. Detected error history – regulators/tax authorities/customers/others
- 7. Detected error history – internal audit
- 8. Detected/known errors in other companies in the same business sector
- 9. Amount of management judgment/subjectivity
- 10. Importance of account/location to security analysts
- 11. Importance of account/note disclosure to debt covenants
- 12. Susceptibility of account to fraud from insiders
- 13.Susceptibility of account to fraud from outsiders
- 14. Account/note linkage to the company's reward/compensation system

Reporting to CEO/Board

Concise reporting on which financial statement line items have the highest residual risk status/high uncertainty

Current assets:		
Cash and cash equivalents	$	20,289
Short-term marketable securities		53,892
Accounts receivable, less allowances of $58 and $53, respectively		17,874
Inventories		4,855
Vendor non-trade receivables		17,799
Other current assets		13,936
Total current assets		128,645
Long-term marketable securities		194,714
Property, plant and equipment, net		33,783
Goodwill		5,717
Acquired intangible assets, net		2,298
Other non-current assets		10,162
Total assets	$	375,319
LIABILITIES AND SHAREHOLDERS' EQUITY:		
Current liabilities:		
Accounts payable	$	49,049
Accrued expenses		25,744
Deferred revenue		7,548
Commercial paper		11,977
Current portion of long-term debt		6,496
Total current liabilities		100,814
Deferred revenue, non-current		2,836
Long-term debt		97,207
Other non-current liabilities		40,415
Total liabilities		241,272
Commitments and contingencies		
Shareholders' equity:		
Common stock and additional paid-in capital, $0.00001 par value: 12,600,000 shares authorized; 5,126,201 and 5,336,166 shares issued and outstanding, respectively		35,867
Retained earnings		98,330
Accumulated other comprehensive income/(loss)		(150)

RISK OVERSIGHT SOLUTIONS

Benefits of Objective Centric Assurance for SOX and SOX like requirements

BENEFITS

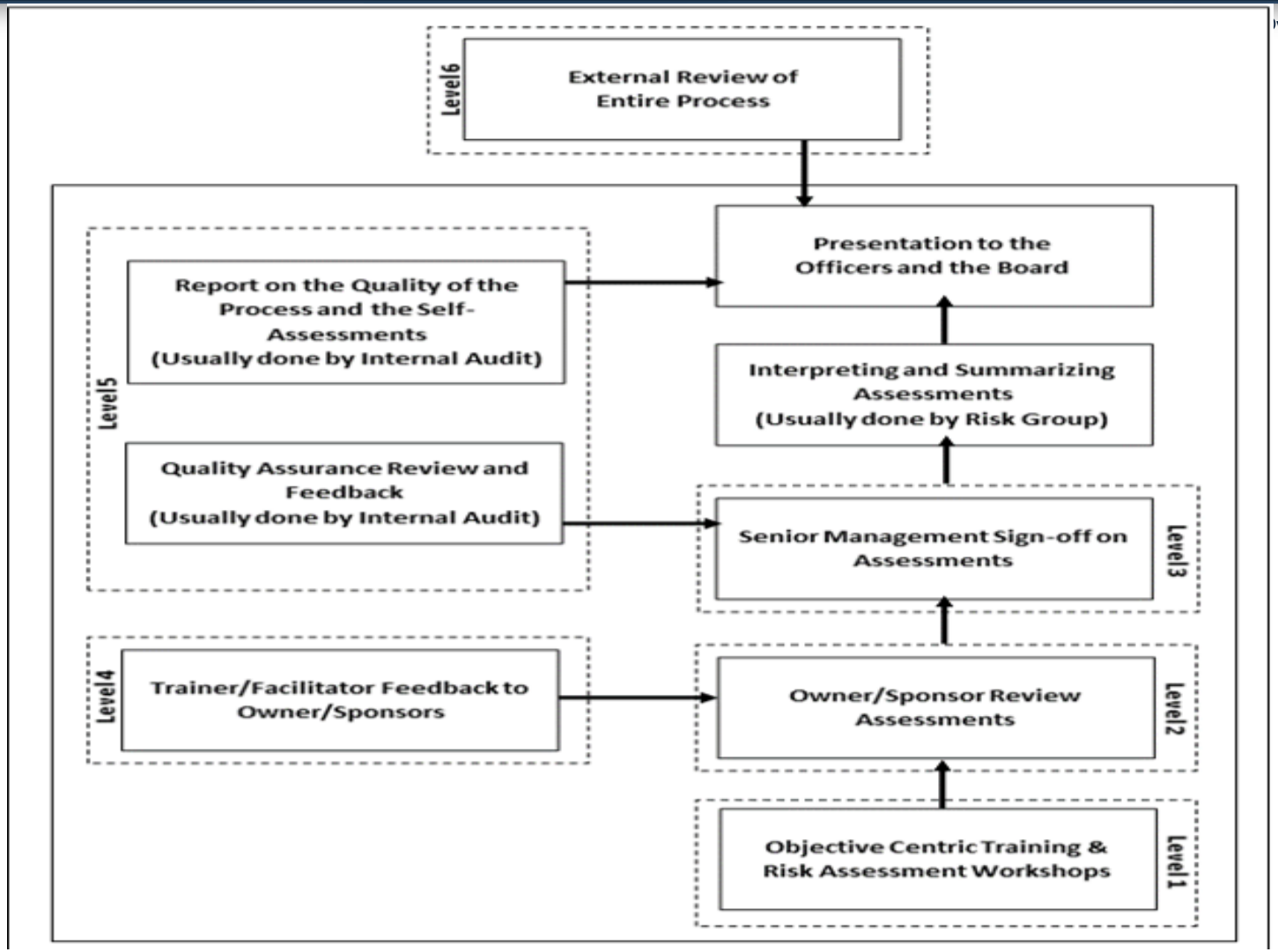
1. Complies with COSO requirement to determine whether there is “an effective system provides reasonable assurance regarding achievement of an entity’s objectives.”
2. Management alerts external auditors to areas with highest residual risk/uncertainty so they can better focus their audit work.
3. This process puts high focus on identification/assessment of risks to help determine resources that should be dedicated to risk treatment design. Current methods often put most time on control testing with limited effort to identify/size risks.

Benefits of Objective Centric Assurance for SOX and SOX like requirements

BENEFITS

4. Lays a foundation to fully integrate work done to ensure financial statements are reliable with ERM work on the full range of value creation and preservation objectives.
5. Uses a wide range of methods to identify risks, current risk treatments and risk treatments that could be used but aren't currently by many companies.
6. Residual risk status/uncertainty information helps management and the board assess if current assurance/uncertainty is "reasonable"/sufficient.
7. The Six Level Quality Assurance framework is able to provide high assurance risk/certainty status information is reliable. See next page.

Benefits of Objective Centric Assurance for SOX and SOX like requirements



OCRCM Overview

QUESTIONS???

Thank you

timleech@riskoversightsolutions.com

RISK OVERSIGHT
SOLUTIONS

Using Objective Centric Risk Assessment for SOX 404 and SOX 404 like requirements

Tim Leech, Managing Director
Risk Oversight Solutions Inc.
timleech@riskoversightsolutions.com

www.riskoversightsolutions.com