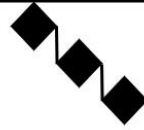

RISK OVERSIGHT

SOLUTIONS



Strong 1st Line/Objective Centric Risk and Uncertainty Management Overview & Business Case

Tim Leech, Managing Director

Risk Oversight Solutions Inc.

timleech@riskoversightsolutions.com

www.riskoversightsolutions.com

Module Coverage

© Risk Oversight Solutions Inc.

Strong 1st Line/Objective Centric Risk & Uncertainty Management (OCRUM) Overview & Business Case

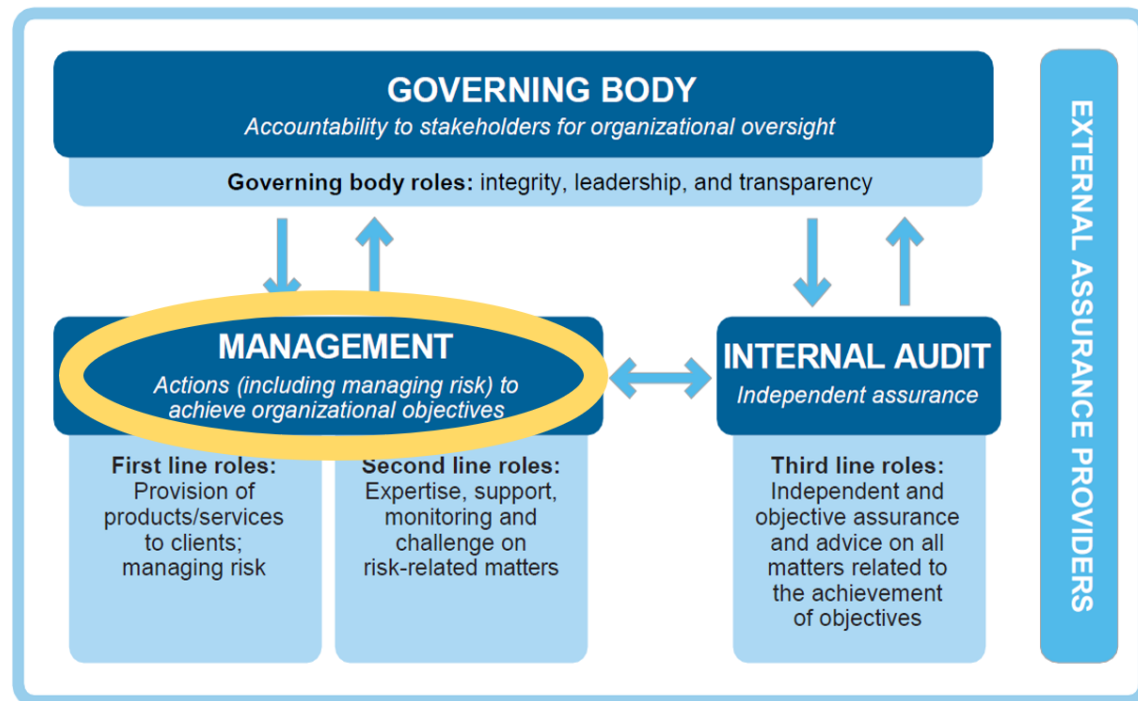
- OCRUM Goals
- OCRUM Core Elements
- OCRUM Management Benefits
- OCRUM Board Benefits
- OCRUM Internal Audit Benefits
- OCRUM Risk Management Benefits
- Measuring Success

OCRUM Goals

© Risk Oversight Solutions Inc.

Re-position primary responsibility for formal risk/uncertainty assessment and reporting from 2nd/3rd Lines to 1st Line - “Strong 1st Line Risk/Uncertainty Management”

The IIA’s Three Lines Model



KEY: ↑ Accountability, reporting ↓ Delegation, direction, resources, oversight ↔ Alignment, communication coordination, collaboration

OCRUM Goals

© Risk Oversight Solutions Inc.

Put equal focus on strategy/value creation and value preservation objectives with clear links to performance in line with COSO ERM 2017 and institutional investor demands



Source: COSO Enterprise Risk Management: Integrating with Strategy and Performance 2017

OCRUM Goals

© Risk Oversight Solutions Inc.

Transition 2nd line risk functions and 3rd line Internal Audit from “supply driven” to “demand driven” service functions with clarity on what CEOs and Boards really need/want from RM/IA



OCRUM Goals

© Risk Oversight Solutions Inc.

Produce dramatically better risk/uncertainty status information to help management and the board make better resource allocation decisions

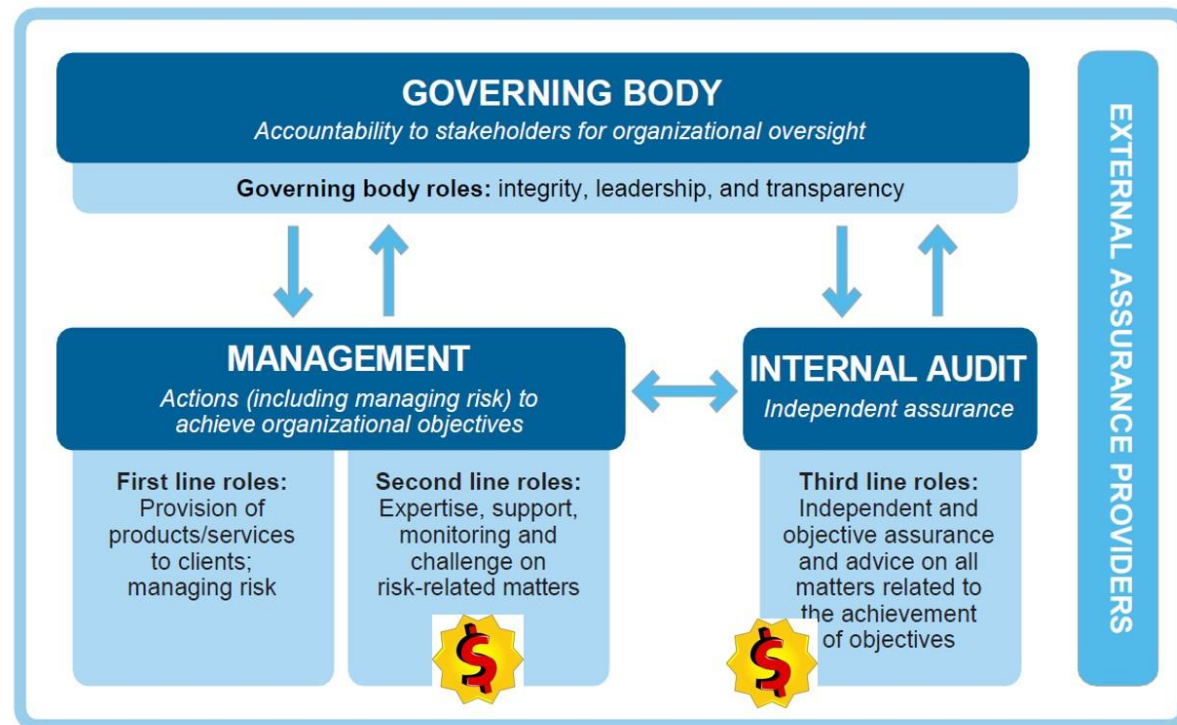


OCRUM Goals

© Risk Oversight Solutions Inc.

Increase the value added from money spent on 2nd and 3rd line functions/staff

The IIA's Three Lines Model



KEY: ↑ Accountability, reporting ↓ Delegation, direction, resources, oversight ↔ Alignment, communication coordination, collaboration

OCRUM Goals

© Risk Oversight Solutions Inc.

Better respond to regulators who want assurance an “effective risk appetite framework” is in place/operating

Post 2008 Global Financial Crisis conclusions:

- **the failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm;**
- compensation programs that conflicted with the control objectives of the firm;
- inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement; and
- institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel.

Source: Senior Supervisors Group Summary Observations Post 2008, Bank for International Settlements October 2009

OCRCM Goals

© Risk Oversight Solutions Inc.

Respond to regulators/stakeholders who want assurance on corporate governance, including board oversight of strategy and risk

Source: OSFI Corporate
Governance Guide
Sept 2018

Table of Contents

- [I. Purpose and Scope of the Guideline](#)
- [II. The Board of Directors](#)
 - [The Role of the Board](#)
 - [The Board and Senior Management](#)
 - [The Board and the Oversight Functions](#)
 - [Boards of Subsidiaries or with FRFI Subsidiaries](#)
 - [Board Effectiveness](#)
- [III. Risk Governance](#)
 - [General](#)
 - [Risk Appetite Framework](#)
 - [Oversight of Risk](#)
- [IV. The Role of the Audit Committee](#)
- [V. Supervision of FRFIs](#)
 - [The Role of Corporate Governance in OSFI's Supervisory Process](#)
 - [OSFI's Supervisory Assessment](#)
 - [Changes to the Board or Senior Management](#)
- [Annex A – The Special Nature of Financial Institutions](#)
- [Annex B – Risk Appetite Framework](#)

OCRUM Goals

© Risk Oversight Solutions Inc.

Respond to powerful institutional investors who want better/more board oversight of strategic planning and risk management



OCRUM Core Elements

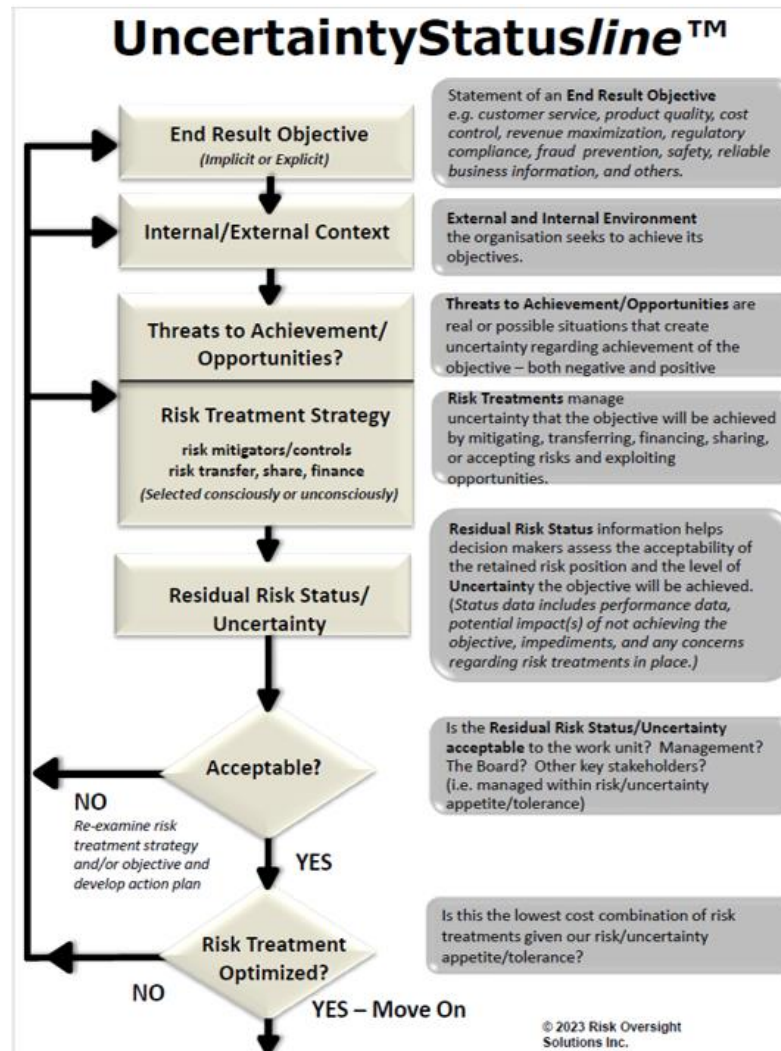
Objective Centric Risk and Uncertainty Management Five Step Overview



OCRUM Core Elements

© Risk Oversight Solutions Inc.

UncertaintyStatusline© is the foundation building block



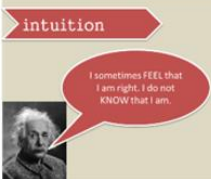



OCRUM Core Elements

© Risk Oversight Solutions Inc.

Conscious and transparent decisions on Risk/Uncertainty Assessment Rigor

Risk Assessment Rigour ("RAR") User Guide

RAR LEVEL	DESCRIPTION
Not Assigned (NA)	
Not Rated (NR)	
Intuitive/Experiential	
Traffic Light/Time Limited	
Full Risk/Risk Treatment Assessment	More work and time required to identify risks, risk treatments, RESIDUAL RISK STATUS information, and COMPOSITE RESIDUAL RISK RATING.
High (H)	Quite a bit more work and time reserved for very important objectives
Very High (VH)	A lot of work and time required reserved for absolutely the most important objectives.
Very High + (VH+)	This amount of effort and time is reserved for situation where there is a desire to be as certain as humanly possible.

OCRUM Core Elements

© Risk Oversight Solutions Inc.

Conscious and transparent decisions on “Independent Assurance Level”

NIA – No independent assurance

LOW – A high level assurance review has been completed and a feedback report provided to the OWNER/SPONSOR and STRATEGY AND VALUE OVERSIGHT COMMITTEE

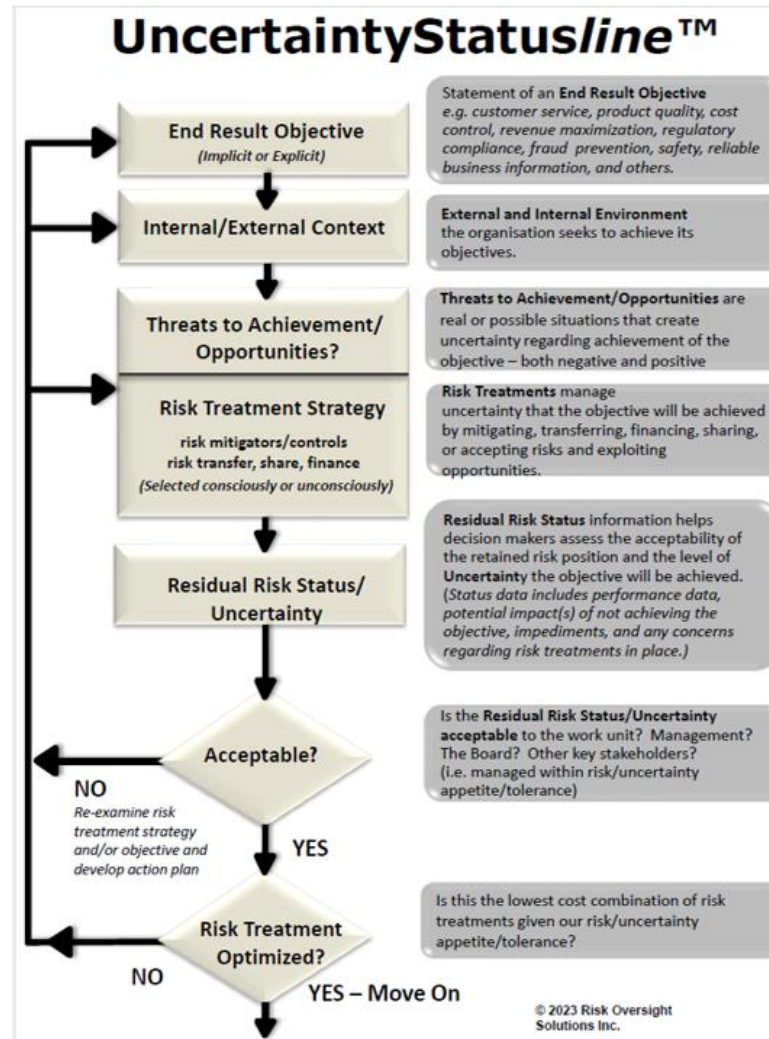
MEDIUM – An independent review has been completed to assess the completeness of risks identified, assessment of those risks, risk treatments and residual risk/uncertainty status information and a report provided to the OWNER/SPONSOR and STRATEGY AND VALUE OVERSIGHT COMMITTEE

HIGH – In addition to the steps defined for MEDIUM, steps have been taken to confirm facts re risk assessments, existence and effectiveness of risk treatments and performance/impact/impediment data.

OCRCM Core Elements

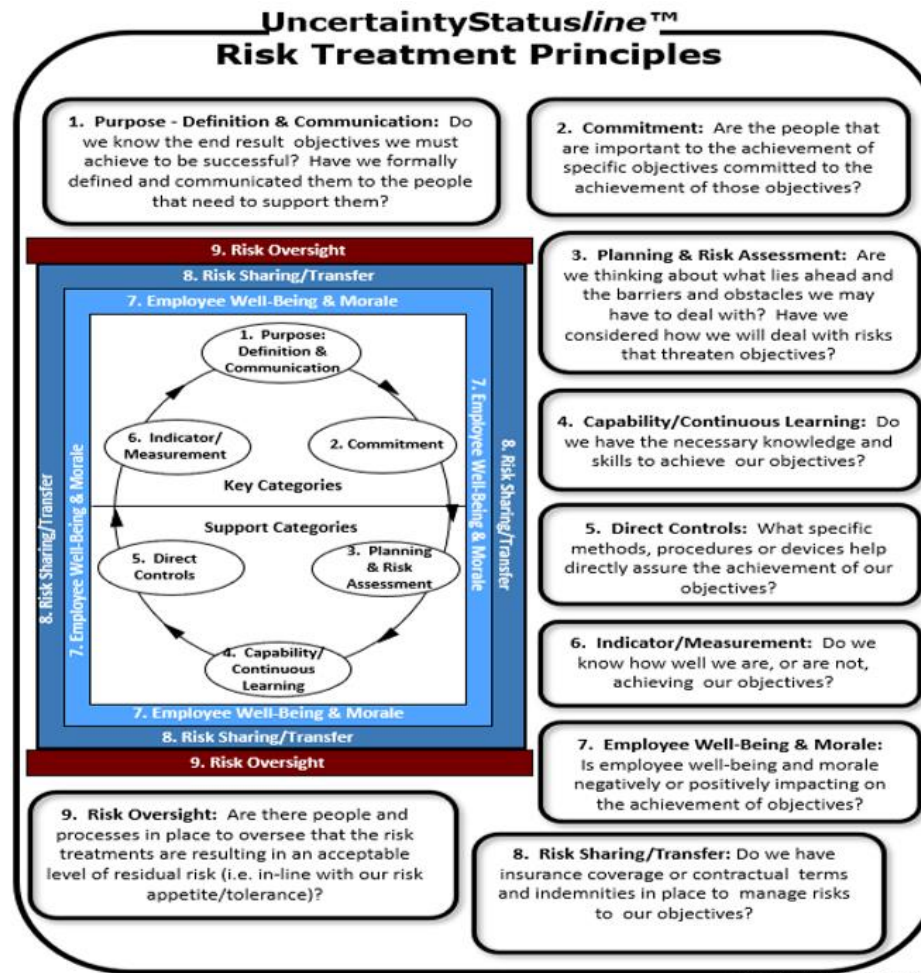
© Risk Oversight Solutions Inc.

Consider the full range of “Risk Treatments” when completing Risk Treatment Strategy section



OCRUM Core Elements

Consider the full range of “Risk Treatments” when completing Risk Treatment Strategy section



OCRUM Core Elements

© Risk Oversight Solutions Inc.

Consider the full range of “Risk Treatments” when completing Risk Treatment Strategy section


Risk Treatment Principles Elements

1. PURPOSE: DEFINITION & COMMUNICATION	5. DIRECT CONTROLS
1.1 Definition of Corporate Mission & Vision	5.1 Direct Controls Related to Business Systems
1.2 Definition of Entity Wide Objectives	5.2 Physical Safeguarding Mechanisms
1.3 Definition of Unit Level Objectives	5.3 Reconciliations/Comparisons/Edits
1.4 Definition of Activity Level Objectives	5.4 Validity/Existence Tests
1.5 Communication of Business/Quality Objectives	5.5 Restricted Access
1.6 Definition and Communication of Corporate Conduct Values and Standards	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
2. COMMITMENT	6. INDICATOR/MEASUREMENT
2.1 Accountability/Responsibility Mechanisms	6.1 Results & Status Reports/Reviews
2.1a Job Descriptions	6.2 Analysis: Statistical/Financial/Competitive
2.1b Performance Contracts/Evaluation Criteria	6.3 Self-Assessments/Direct Report Audits
2.1c Budgeting/Forecasting Processing	6.4 Benchmarking Tools/Processes
2.1d Written Accountability Acknowledgements	6.5 Customer Survey Tools/Processes
2.1e Other Accountability/Responsibility Mechanisms	6.6 Automated Monitoring/Reporting Mechanisms & Reports
2.2 Motivation/Reward/Punishment Mechanisms	6.7 Integrity Concerns Reporting Mechanisms
2.2a Performance Evaluation System	6.8 Employee/Supervisor Observation
2.2b Promotion Practices	6.9 Other Indicator/Measurement Controls
2.2c Firing and Discipline Practices	
2.2d Reward Systems - Monetary	7. EMPLOYEE WELL-BEING & MORALE
2.2e Reward Systems - Non-Monetary	7.1 Employee Surveys
2.3 Organization Design	7.2 Employee Focus Groups
2.4 Self-Assessment/Risk Acceptance Processes	7.3 Employee Question/Answer Vehicles
2.5 Officer/Board Level Review	7.4 Management Communication Processes
2.6 Other Commitment Controls	7.5 Personal and Career Planning
	7.6 Diversity Training/Recognition
3. PLANNING & RISK ASSESSMENT	7.7 Equity Analysis Processes
3.1 Strategic Business Analysis	7.8 Measurement Tools/Processes
3.2 Short, Medium and Long Range Planning	7.9 Other Well-Being/Morale Processes
3.3 Risk Assessment Processes - Macro Level	
3.4 Risk Assessment Processes - Micro Level	8. RISK SHARING/TRANSFER
3.5 Control & Risk Self-Assessment	8.1 Insurance Coverage
3.6 Continuous Improvement & Analysis Tools	8.2 Contractual Indemnities/Remediation
3.7 Systems Development Methodologies	8.3 Civil Law Recovery
3.8 Disaster Recovery/Contingency Planning	8.4 Other Risk Sharing/Transfer Vehicles
3.9 Other Planning & Risk Assessment Processes	
	9. RISK OVERSIGHT
4. CAPABILITY/CONTINUOUS LEARNING	9.1 Manager/Officer Monitoring/Supervision
4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes	9.2 Internal Audits
4.2 Self-Assessment Forums & Tools	9.3 External Audits
4.3 Coaching/Training Activities & Processes	9.4 Specialist Reviews & Audits
4.4 Hiring and Selection Procedures	9.5 ISO Review/Regulator Inspections
4.5 Performance Evaluation	9.6 Audit Committee/Board Oversight
4.6 Career Planning Processes	9.7 Self-Assessment Quality Assurance Reviews
4.7 Firing Practices	9.8 Authority Grids/Structures & Procedures
4.8 Reference Aids	9.9 Other Risk Oversight Activities
4.9 Other Training/Education Methods	

OCRUM Core Elements

© Risk Oversight Solutions Inc.

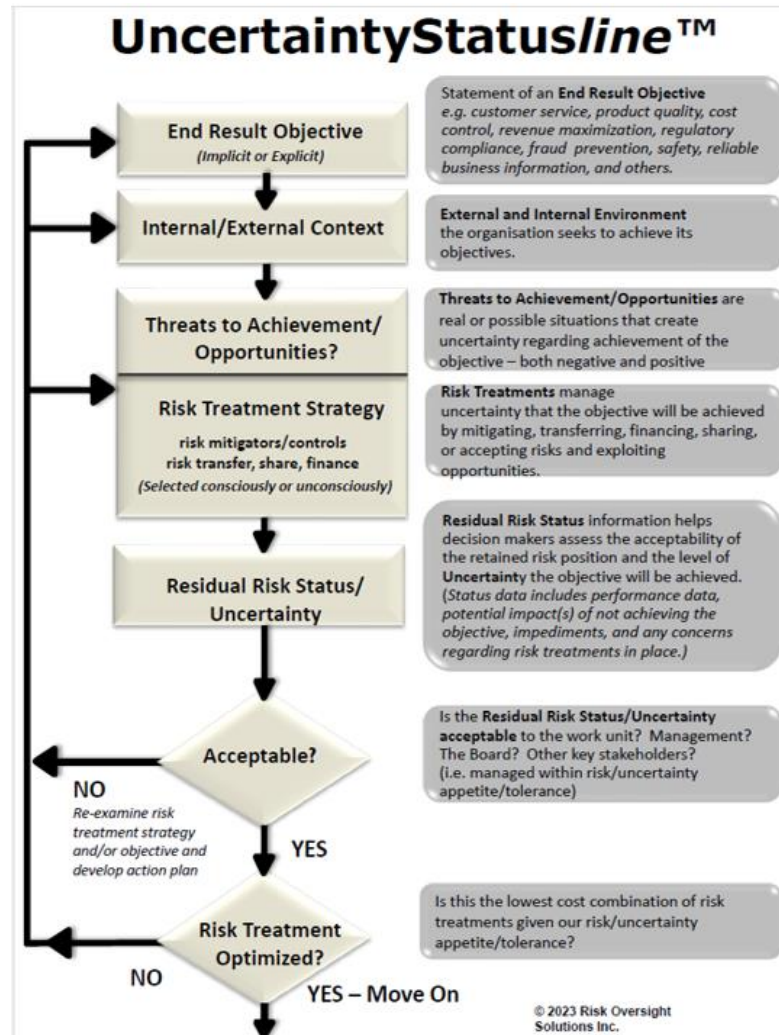
Uncertainty Ratings (URs)



Fully acceptable level of uncertainty of achievement. Any significant concerns have been identified and shared upwards
Some management effort is required to reduce uncertainty of achievement to an acceptable level.
Considerable management action is required to reduce uncertainty of achievement to an acceptable level.
Significant analysis and corrective action by Senior Management and the Board is urgently required to reduce uncertainty of achievement to an acceptable level.
Massive corrective action by Senior Management and the Board is required now to reduce uncertainty of achievement to an acceptable level.

OCRUM Core Elements

After the decision on acceptability of residual risk status/uncertainty has been made, assess if the Risk Treatment Strategy is “Optimized” © Risk Oversight Solutions Inc.



OCRUM Core Elements

© Risk Oversight Solutions Inc.

Provide consolidated reports on residual risk status/uncertainty linked to key objectives



Uncertainty Ratings (URs)

Fully acceptable level of uncertainty of achievement. Any significant concerns have been identified and shared upwards

Some management effort is required to reduce uncertainty of achievement to an acceptable level.

Considerable management action is required to reduce uncertainty of achievement to an acceptable level.

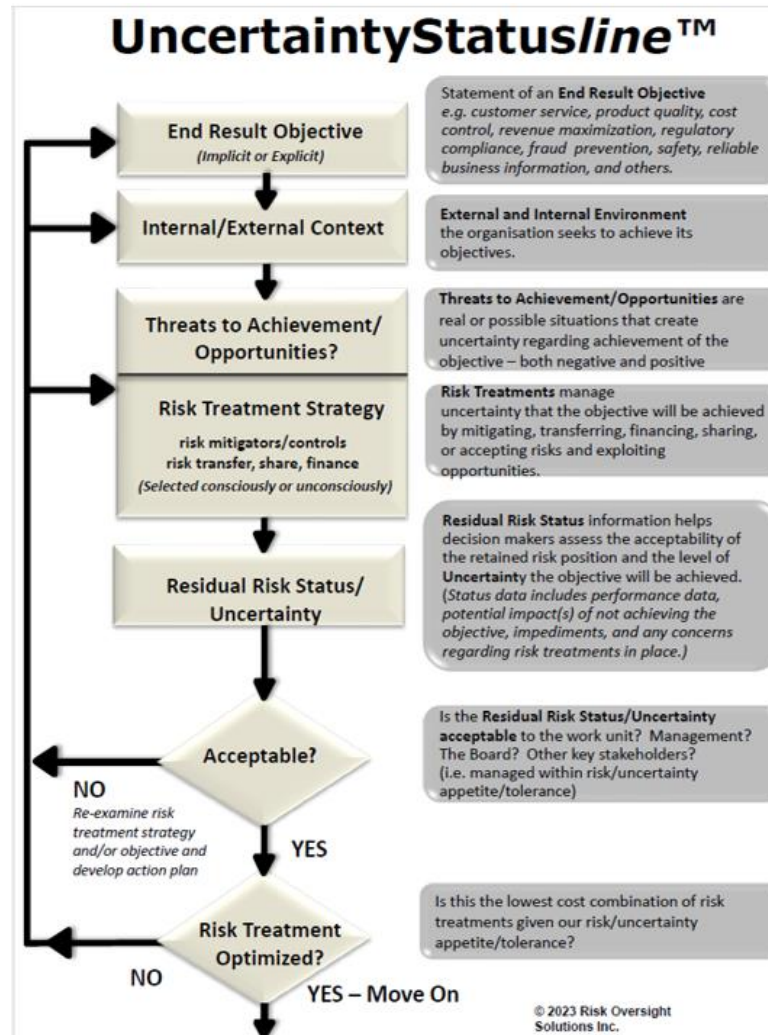
Significant analysis and corrective action by Senior Management and the Board is urgently required to reduce uncertainty of achievement to an acceptable level.

Massive corrective action by Senior Management and the Board is required now to reduce uncertainty of achievement to an acceptable level.

OCRUM Core Elements

After the decision on acceptability of residual risk status/uncertainty has been made, assess if the Risk Treatment Strategy is “Optimized”

© Risk Oversight Solutions Inc.



OCRUM Top Management Benefits

© Risk Oversight Solutions Inc.

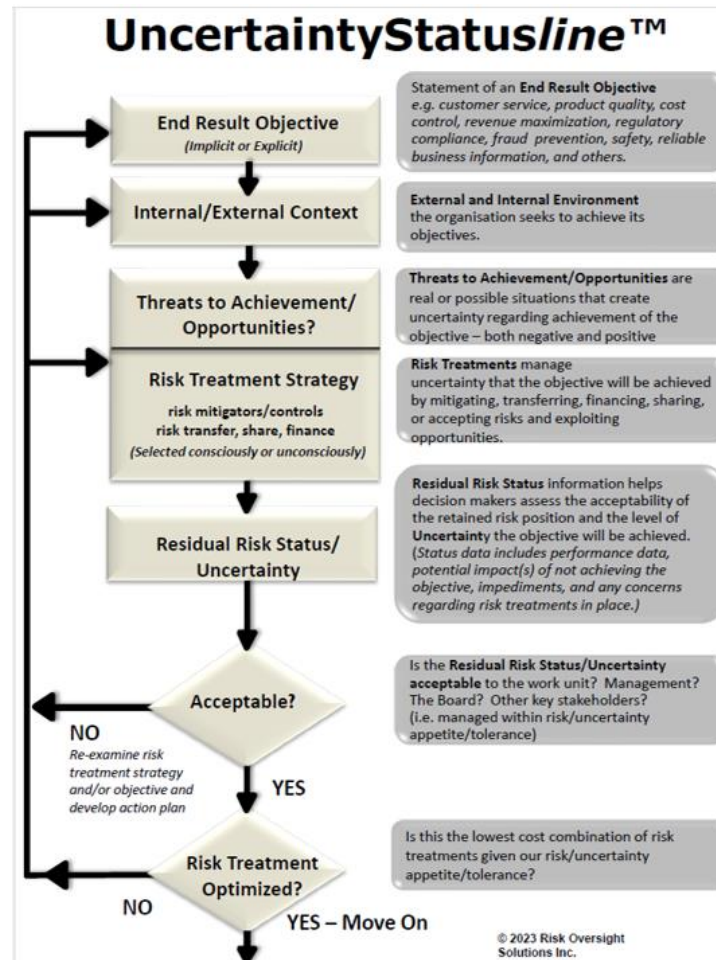
More confidence key objectives will be achieved with acceptable level of risk



OCRUM Top Management Benefits

© Risk Oversight Solutions Inc.

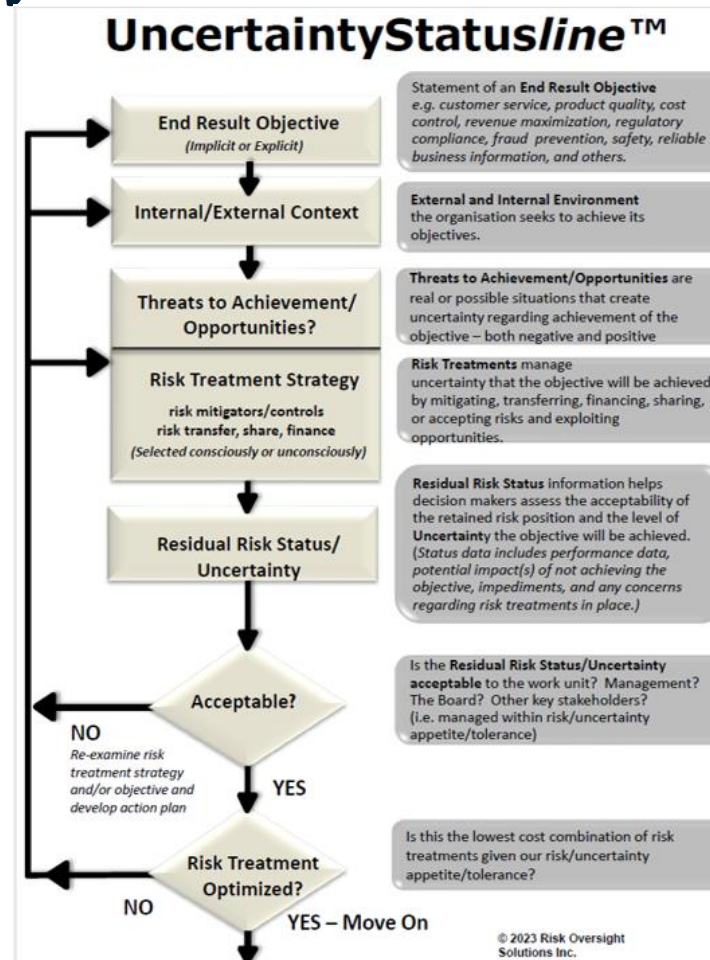
Management can see the relationship between risks/risk treatments/residual risk and performance



OCRUM Top Management Benefits

© Risk Oversight Solutions Inc.

Management makes a conscious decision on acceptability of current risk/uncertainty

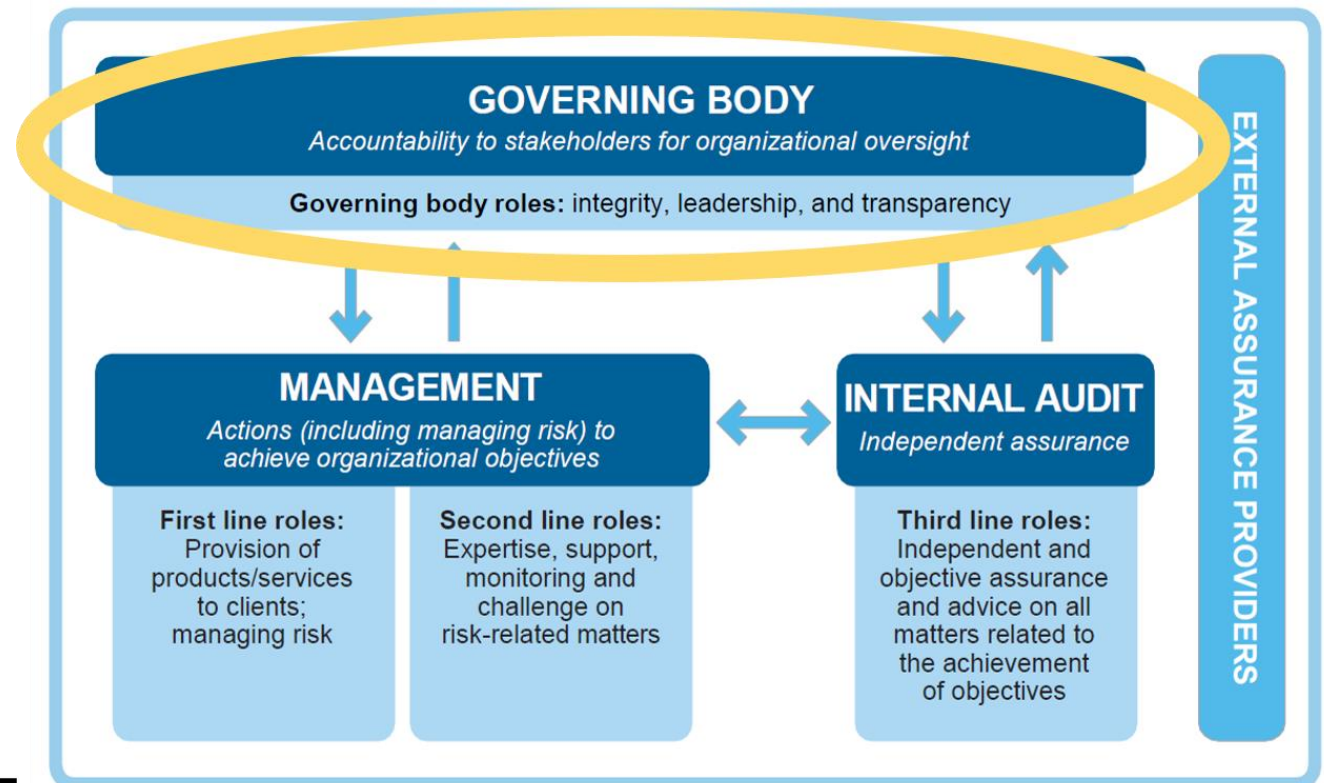


OCRUM Top Board Benefits

© Risk Oversight Solutions Inc.

Boards are better positioned to meet stakeholder risk governance expectations

The IIA's Three Lines Model



OCRUM Top Board Benefits

© Risk Oversight Solutions Inc.

Boards get concise reports on uncertainty linked to “mission critical” objectives



Uncertainty Ratings (URs)

Fully acceptable level of uncertainty of achievement. Any significant concerns have been identified and shared upwards

Some management effort is required to reduce uncertainty of achievement to an acceptable level.

Considerable management action is required to reduce uncertainty of achievement to an acceptable level.

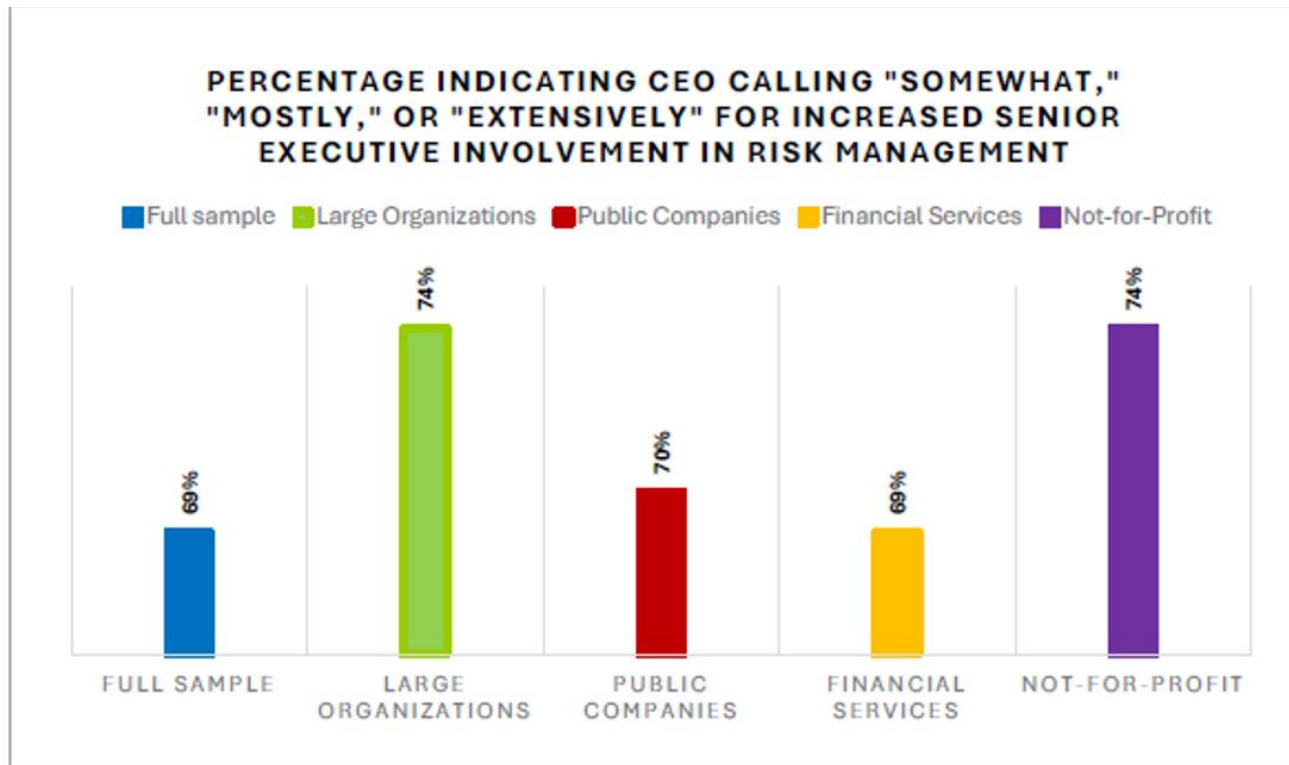
Significant analysis and corrective action by Senior Management and the Board is urgently required to reduce uncertainty of achievement to an acceptable level.

Massive corrective action by Senior Management and the Board is required now to reduce uncertainty of achievement to an acceptable level.

OCRUM Top Board Benefits

© Risk Oversight Solutions Inc.

Boards get what they have been saying for 5 years they want from senior management



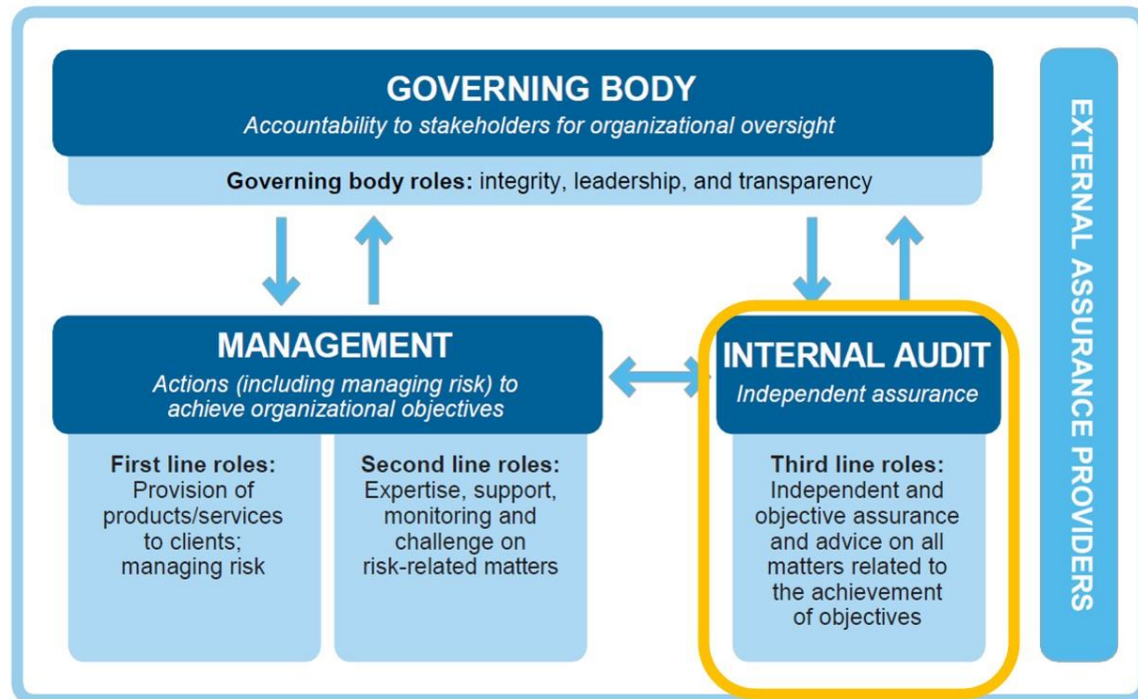
2024 THE STATE OF RISK OVERSIGHT:
AN OVERVIEW OF ENTERPRISE RISK PRACTICES

OCRUM Internal Audit Benefits

© Risk Oversight Solutions Inc.

Internal audit services are “demand driven” not “supply driven”. IA resourcing/staffing is linked directly to Board/CEO requirements

The IIA's Three Lines Model



OCRUM Internal Audit Benefits

© Risk Oversight Solutions Inc.

Counterproductive conflict with management is reduced.
 Management can take any level of risk they think is appropriate as long as they are prepared to share risk/uncertainty status with those above them.



Uncertainty Ratings (URs)

Fully acceptable level of uncertainty of achievement. Any significant concerns have been identified and shared upwards

Some management effort is required to reduce uncertainty of achievement to an acceptable level.

Considerable management action is required to reduce uncertainty of achievement to an acceptable level.

Significant analysis and corrective action by Senior Management and the Board is urgently required to reduce uncertainty of achievement to an acceptable level.

Massive corrective action by Senior Management and the Board is required now to reduce uncertainty of achievement to an acceptable level.

OCRUM Internal Audit Benefits

© Risk Oversight Solutions Inc.

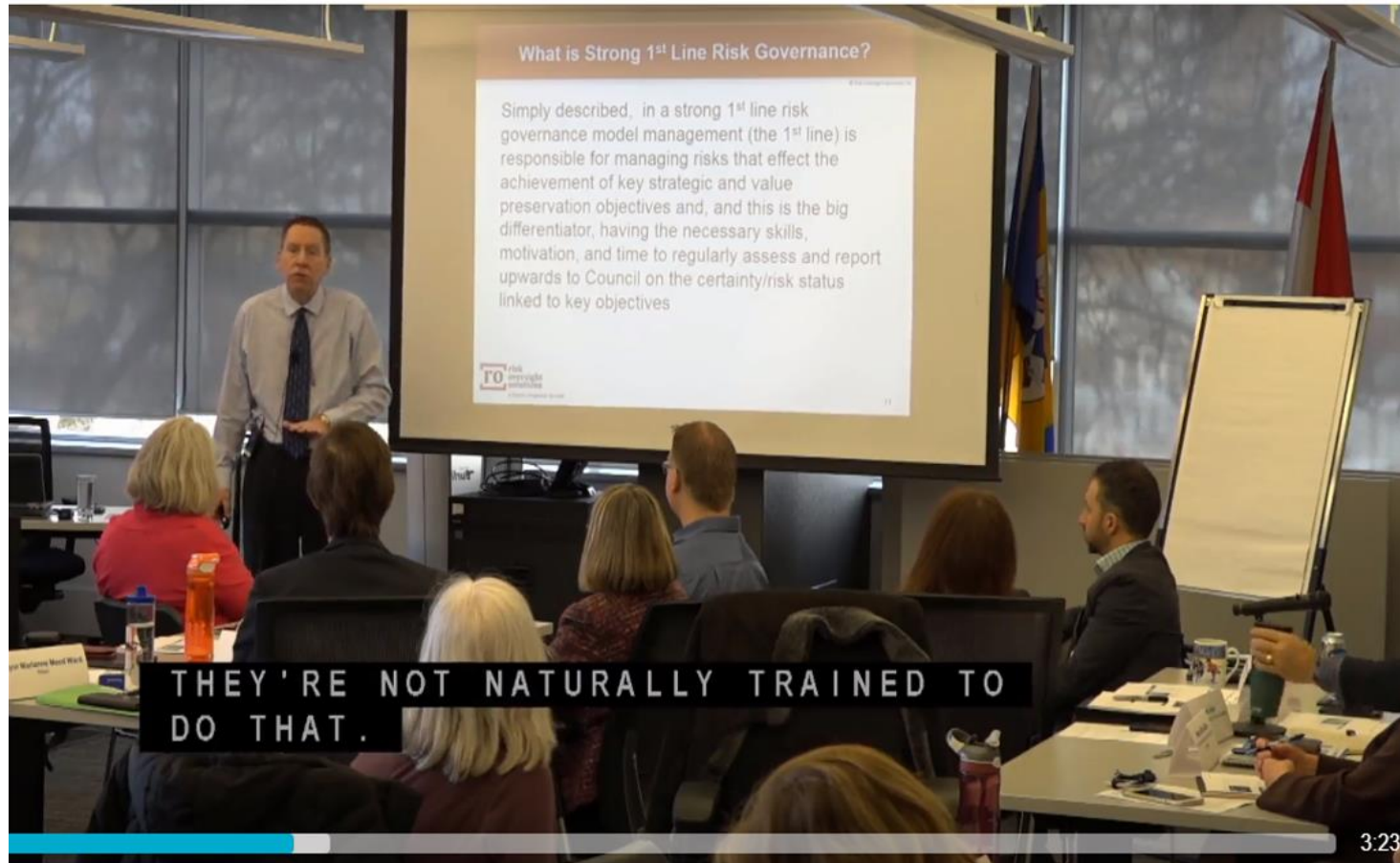
Internal audit is focused on helping management increase certainty the most important “mission critical” objectives, including strategic objectives, are achieved while operating with an acceptable level of residual risk status/uncertainty



OCRUM Internal Audit Benefits

© Risk Oversight Solutions Inc.

Internal audit staff learn skills that will be incredibly valuable in any future management/IA/RM positions



OCRCM Risk Management Benefits

© Risk Oversight Solutions Inc.

RM resources are focused on helping management increase certainty “Mission Critical” objectives are achieved with acceptable levels of residual risk/uncertainty

Board Oversight 2021: “Mission Critical” Risks and the Corporate “Mission” Converge

By Adé Heyliger, Lyuba Goltser, and Ellen Odoner, Weil, Gotshal & Manges¹

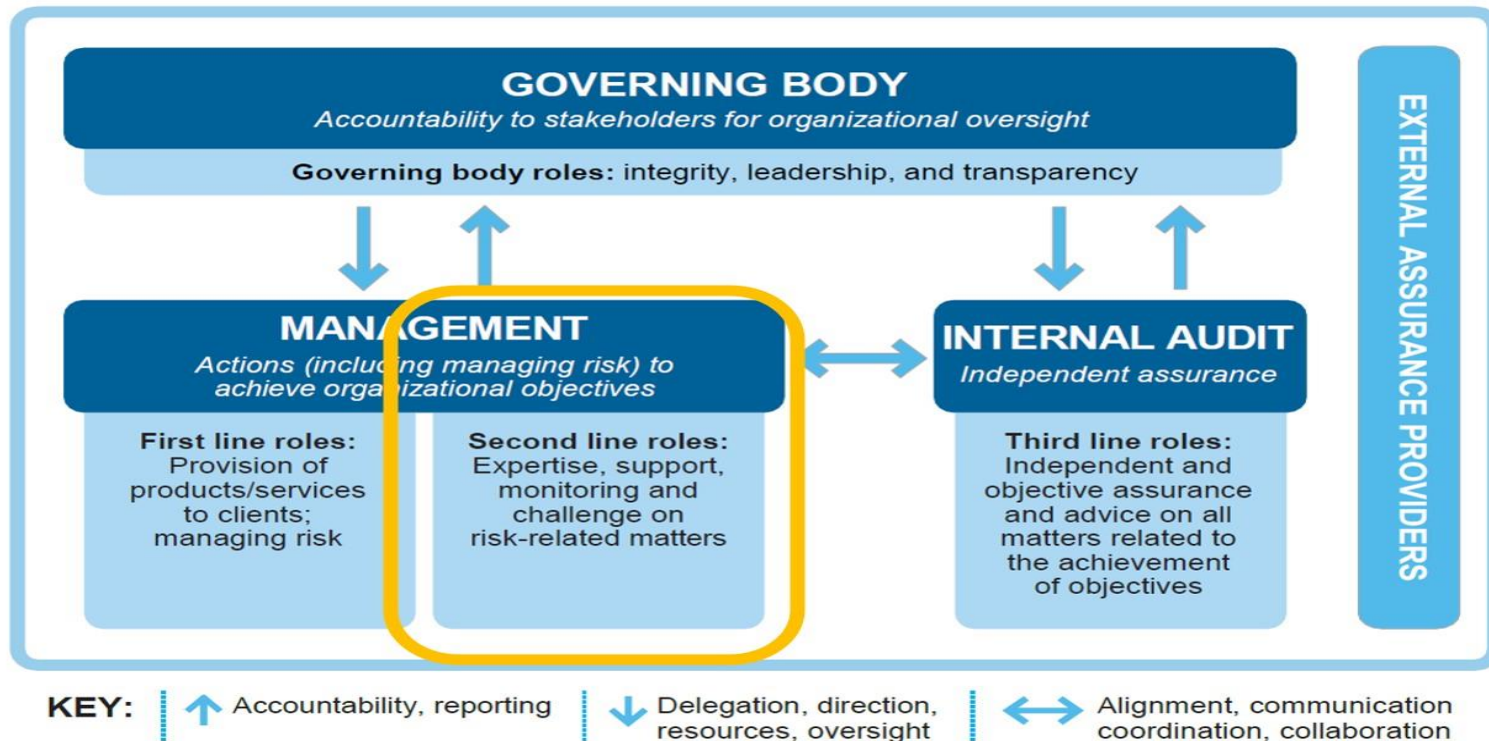


OCRUM Risk Management Benefits

© Risk Oversight Solutions Inc.

Risk management resourcing is determined by board/CEO requirements for reliable risk/uncertainty status information from Owner/Sponsors linked to mission critical objectives

The IIA's Three Lines Model



OCRUM Risk Management Benefits

© Risk Oversight Solutions Inc.

In highly regulated sectors 2nd line work directly supports meeting regulatory expectations the company is operating within acceptable risk appetite/tolerance boundaries

Table of Contents

- [I. Purpose and Scope of the Guideline](#)
- [II. The Board of Directors](#)
 - [The Role of the Board](#)
 - [The Board and Senior Management](#)
 - [The Board and the Oversight Functions](#)
 - [Boards of Subsidiaries or with FRFI Subsidiaries](#)
 - [Board Effectiveness](#)
- [III. Risk Governance](#)
 - [General](#)
 - [Risk Appetite Framework](#)
 - [Oversight of Risk](#)
- [IV. The Role of the Audit Committee](#)
- [V. Supervision of FRFIs](#)
 - [The Role of Corporate Governance in OSFI's Supervisory Process](#)
 - [OSFI's Supervisory Assessment](#)
 - [Changes to the Board or Senior Management](#)
- [Annex A – The Special Nature of Financial Institutions](#)
- [Annex B – Risk Appetite Framework](#)

Measuring Success

© Risk Oversight Solutions Inc.

Tim's view - "effective risk management" provides C-Suite and Board with a materially reliable picture of the risk/uncertainty status of achieving MISSION CRITICAL OBJECTIVES. Few RM/IA functions do that today = Level 5 "Optimized" RM per IIA.

5 – Optimized

Risk appetite	Once the risk appetite has been approved by the board, management and key employees implement it throughout the organization in a format and level of detail appropriate for decision-making.
Risk assessment	Management uses a common process to conduct risk assessments, document risk information, and monitor its performance against risk-adjusted KPIs. Management has protocols in place to ensure that significant risks are addressed when they arise, rather than during or after next scheduled risk assessment.
Common language	The entire organization, from the board to line/operational management and employees, has a common understanding of the terms used in the risk management process (e.g., risk, contributing factor, control, impact, likelihood) and uses a common language to discuss risk.
Use of risk information	Risks are tied to the organization's objectives at every level. Further, risk information is communicated throughout the organization on an ongoing basis, and compensation and incentives for management are linked to KPIs driven by identified and assessed risks.

QUESTIONS???

Thank you

timelech@riskoversightsolutions.com