IS INTERNAL AUDIT THE NEXT BLACKBERRY? IT REALLY IS TIME TO REINVENT THE PROFESSION

IIA CANADA WEBINAR
MARCH 14, 2017

TIM LEECH FCPA CIA CRMA CCSA CFE
RISK OVERSIGHT SOLUTIONS INC.
TIMLEECH@RISKOVERSIGHTSOLUTIONS.COM
Tim J. Leech, FCPA CIA CRMA CCSA CFE is Managing Director at Risk Oversight Solutions Inc. based in Oakville, Ontario, Canada and Sarasota, Florida. He has over 30 years of experience in the risk governance, internal audit, IT, and forensic accounting/litigation support fields. His experience base includes setting up a new business unit, a “first of its kind”, for Coopers & Lybrand, “Control & Risk Management Services” in 1987; founding in 1991, building, and successfully selling CARD®decisions, a global risk and assurance consulting and software firm, to Paisley/Thomson Reuters in 2004; serving as Paisley’s Chief Methodology Officer from 2004 -2007; and 30+ years of global experience helping clients around the world with internal audit transformation initiatives and the design, implementation, and maintenance of integrated and more powerful ERM/IA methodology and technology frameworks.

He developed and successfully released CARD®map, the world’s first integrated risk and assurance software, in 1997. The web-enabled “cloud” version of CARD®map was released in 2000. Tim was the first in 2009 to develop and deliver training on IIA IPPF Standard 2120 to equip internal auditors to assess and report on the effectiveness of risk management processes. He is the author of the Conference Board Director Notes December 2012 publication “Board Oversight of Management’s Risk Appetite and Tolerance”, co-author of the highly acclaimed January 2014 “Risk Oversight: Evolving Expectations for Boards”, and author of the provocative “Paradigm Paralysis in ERM and Internal Audit” in the summer 2016 issue of Ethical Boardroom. His ground breaking article, “Reinventing Internal Audit”, published in the April 2015 issue of Internal Auditor magazine, has attracted global recognition and was awarded a 2016 Outstanding Contribution Award from IIA global. His article “Is Internal Audit the Next Blackberry?” published in the ACCA Internal Audit Bulletin has received global accolades and recognition. His newest article “Focusing ERM and Internal Audit on What Really Matters: Long term value creation and preservation” will appear in the spring issue of Ethical Boardroom in April 2017.

In 2016 he launched a second generation of disruptive innovation with a breakthrough approach to risk and assurance management – “Objective Centric ERM and Internal Audit”. The goal – respond to the rapid escalation in board risk oversight expectations, a rapid deterioration in customer satisfaction with traditional ERM/IA approaches, and deliver substantially more “bang for the buck” from formal assurance spending.
What is “Paradigm Paralysis”?  
Paradigm paralysis: ERM  
Paradigm paralysis: Internal Audit (IA)  
Who is most negatively impacted by ERM/IA paralysis?  
Who could drive positive change?  
Barriers to change  
The way forward: OBJECTIVE CENTRIC ERM AND INTERNAL AUDIT (OCERM/IA)  
OCERM/IA: The business case  
OCERM/IA: Implementation options  
Questions
What is paradigm paralysis? Or more basically, what is a paradigm?

As you probably know, a paradigm is a model or a pattern. It's a shared set of assumptions that have to do with how we perceive the world.

Paradigms are very helpful because they allow us to develop expectations about what will probably occur based on these assumptions. But when data falls outside our paradigm, we find it hard to see and accept. This is called the PARADIGM EFFECT. And when the paradigm effect is so strong that we are prevented from actually seeing what is under our very noses, we are said to be suffering from paradigm paralysis.

(Source:https://www.mnsu.edu/comdis/kuster/Infostuttering/Paradigmparalysis.html)
What is “Paradigm Paralysis”?

Internal Audit and ERM: Disturbing parallels with Kodak, Xerox and Blackberry

A survey done by PwC in 2014 indicated only 45% of senior managers believe Internal Audit provides "significant value" and only 49% believe IA performs well. A 2016 AICPA/NCS risk oversight survey found that "Only 25% believe their organization has a “complete formal enterprise-risk management process in place,” and that finding has not risen over the past four years, suggesting that organizations have not made significant strides in risk oversight maturity." Other surveys have produced similar disturbing results on IA and ERM progress. Although this is clearly the "half empty" view of the glass, there is mounting evidence both internal audit and ERM practitioners need to stop and consider if they have the same afflictions that have crippled big name brand companies including Kodak, Blackberry, Yahoo and Xerox. One analysis proposed 9 reasons. The number one reason is failure to innovate. The other 8 reasons are well worth reading (https://goo.gl/lvSbTl). I have proposed that both IA and ERM have a bad case of "paradigm paralysis". (https://goo.gl/KBZdyk)

What do you think it will take to help IA and ERM avoiding the same fate of these companies? Show less
What is “Paradigm Paralysis”?

9 Reasons Kodak, Blackberry, Yahoo, & Other Major Brands Fail

By Scott Williams - May 3, 2012

1. Inability to Innovate
2. Inability to Stay Ahead of the Times
3. No Adjustments
4. Uncle Rico Syndrome
5. The Top Stays the Same
6. Inbred Syndrome
7. Reluctance to Take Risks
8. Refuse to Surround Themselves with and Retain the Best
9. Unwillingness to Change
Polling Question #1

“Paradigm paralysis” is:

a) Something that sometimes happens to older people
b) Something that happened at Kodak, Xerox and Blackberry that contributed to their decline
c) A shared set of assumptions that have to do with how we perceive the world
d) A,B + C
e) A frozen state of mind that drives rapid innovation to better meet customer needs
f) Don’t know
Risk register

From Wikipedia, the free encyclopedia

A risk register (or risk log e.g. in PRINCE2) is a scatterplot used as risk management tool and to fulfill regulatory compliance acting as a repository for all risks identified and includes additional information about each risk, e.g. nature of the risk, reference and owner, mitigation measures.

ISO 27005 Risk management—Vocabulary[8] defines a risk register to be a “record of information about identified risks”.

### Example

Risk register the project “barbecue party” with somebody inexperienced handling the grill, both in table format (below) and as plot (right).

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Probability</th>
<th>Impact</th>
<th>Mitigation</th>
<th>Contingency</th>
<th>Risk Score after Mitigation</th>
<th>Action By</th>
<th>Action When</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guests</td>
<td>The guests find the party boring</td>
<td>1.1</td>
<td>low</td>
<td>medium</td>
<td>invite crazy friends, provide sufficient liquor</td>
<td>Bring out the karaoke</td>
<td>2</td>
<td>within 2hrs</td>
</tr>
<tr>
<td>Guests</td>
<td>Drunken brawl</td>
<td>1.2</td>
<td>medium</td>
<td>low</td>
<td>don’t invite crazy friends, don’t provide too much liquor</td>
<td>Call 911</td>
<td>x</td>
<td>Now</td>
</tr>
<tr>
<td>Nature</td>
<td>Rain</td>
<td>2.1</td>
<td>low</td>
<td>high</td>
<td>have the party indoors</td>
<td>Move the party indoors</td>
<td>0</td>
<td>10mins</td>
</tr>
<tr>
<td>Nature</td>
<td>Fire</td>
<td>2.2</td>
<td>highest</td>
<td>highest</td>
<td>start the party with instructions on what to do in the event of fire</td>
<td>Implement the appropriate response plan</td>
<td>1</td>
<td>Everyone</td>
</tr>
<tr>
<td>Food</td>
<td>Not enough food</td>
<td>3.1</td>
<td>high</td>
<td>high</td>
<td>have a buffer</td>
<td>Order pizza</td>
<td>1</td>
<td>30mins</td>
</tr>
<tr>
<td>Food</td>
<td>Food is spoiled</td>
<td>3.2</td>
<td>high</td>
<td>highest</td>
<td>store the food in deep freezer</td>
<td>Order pizza</td>
<td>1</td>
<td>30mins</td>
</tr>
</tbody>
</table>

### Terminology

A Risk Register can contain many different items. There are recommendations for Risk Register content made by the Project Management Institute Body of Knowledge (PMBOK) and PRINCE2. ISO 31000:2009[8] does not use the term risk register, however it does state that risks need to be documented.

There are many different tools that can act as risk registers from comprehensive software suites to simple spreadsheets. The effectiveness of these tools depends on their implementation and the organisation’s culture.[citation needed]

A typical risk register contains:

- A risk category to group similar risks
- A brief description of the risk, including a possible cause of the risk
- The probability of the event occurring
- The impact of the event
- The risk owner
- The risk mitigation action
- The risk contingency plan
- The risk action by
- The risk action when
What’s wrong with the COSO June 2016 ERM exposure draft?

• LACK OF RESEARCH ON CAUSES OF ERM Failures
• STRADDLING TWO CONFLICTING ERM PARADIGMS
• CONFLICTING GUIDANCE ON ERM AND INTERNAL CONTROL
• LACK OF RECOGNITION AND INTEGRATION WITH ISO 31000 RISK MANAGEMENT STANDARD
• THE ROLE OF INTERNAL AUDIT

Internal audit

From Wikipedia, the free encyclopedia

**Internal auditing** is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.\(^1\) Internal auditing is a catalyst for improving an organization's governance, risk management and management controls by providing insight and recommendations based on analyses and assessments of data and business processes.\(^2\) With commitment to **integrity** and **accountability**, internal auditing provides value to governing bodies and **senior management** as an objective source of independent advice. Professionals called **internal auditors** are employed by organizations to perform the internal auditing activity.

The scope of internal auditing within an organization is broad and may involve topics such as an organization's governance, risk management and management controls over:

- efficiency/effectiveness of operations (including safeguarding of assets), the reliability of financial and management reporting,\(^3\)[4]\ and **compliance** with laws and regulations. Internal auditing may also involve conducting proactive fraud audits to identify potentially fraudulent acts; participating in fraud investigations under the direction of fraud investigation professionals, and conducting post investigation fraud audits to identify control breakdowns and establish financial loss.

Internal auditors are not responsible for the execution of company activities; they **advise** management and the **Board of Directors** (or similar **oversight** body) regarding how to better execute their **responsibilities**. As a result of their broad scope of involvement, internal auditors may have a variety of higher educational and professional backgrounds.
Key Attributes of Traditional “Direct Report” Internal Audit

• Internal audit creates and maintain a “audit universe” – units/topics/things IA believes it could “audit”

• IA complete audits of audit universe elements selected for the year and provide an opinion whether they think “internal controls” in the area examined are “effective” or “deficient”.

• This traditional IA approach is called “direct report” auditing. The person responsible for the area being audited does not make a representation on the state of risk/control/residual risk. If they did, and IA completed an audit of the representation from the responsible person(s), it would be called a “attestation” audit. Financial statement audits done by external auditors are attestation audits. Auditors opine on whether it is reliable, not whether they like it or think it’s not “effective”.
Key Attributes of Traditional “Direct Report” Internal Audit

• Annual coverage is usually less than 5% of the total risk universe

• Coverage frequently does not include the organization’s top value creation objectives (objectives key to the long term success of the enterprise that will create enhanced stakeholder value)

• History indicates the traditional IA approach frequently misses major risks to the organization’s long term success

• Auditees frequently experience pressure to “fix” areas where IA believe internal controls are “ineffective” and relations can be adversarial

• The process can result in sub-optimal entity level resource allocation (i.e. resources are directed to fix areas identified as “deficient” by IA because of board pressure not because they are where resources are most needed)
Polling Question #2

The number one cause of significant declines in internal audit customer satisfaction globally in your opinion is:

a) New board risk oversight expectations - traditional IA methods don’t provide enough help
b) Critical internal audit reports that irritate management
c) Internal audit isn’t delivering what customers need most – help managing rapid change and big risks
d) Not enough focus on effectiveness of risk processes
e) Internal audit isn’t delivering what C-Suite and boards see as sufficient bang for the buck
f) All of the above
g) Other
h) Don’t know
Who is most negatively impacted by ERM/IA paradigm paralysis?

Those impacted by major business failures
Who is most negatively impacted by ERM/IA paradigm paralysis?

Figure 4. Satisfaction with internal audit value and performance

Percent of stakeholders reporting internal audit provides “significant value”

79% 68%

44% 45%

Board Members Senior Management

Percent of 2014 respondents reporting that internal audit “performs well”¹

64% 49% 65%

Board Members Senior Management CAEs

¹Represents the average of “performs well” ratings

Global State of Enterprise Risk Oversight: 2nd Edition

- **60%** of boards of directors in most regions of the world are placing significant pressure on organisations to increase senior management’s involvement in risk oversight.
- **70%** or more of boards in all regions of the world outside the U.S. are formally assigning risk oversight responsibilities to a board committee. Surprisingly, only 46% of U.S. boards are doing so.
- Less than half (42%) of organisations discuss risk information generated by the ERM process when the board discusses the organisation’s strategic plan.
- Over **60%** of organisations in most regions have internal management level risk committees. The exception is in the U.S, where only 44% indicate they have those committees in place.
- Few organisations (around **20%**) integrate risk management activities with performance compensation/remuneration and most (about **80%**) have not invested in risk management training for executives in the past few years.

Global State of Enterprise Risk Oversight: 2nd Edition

• About 60% of organisations worldwide agree that they face a wide array of complex and increasing risk issues.
• Despite that, 35% or fewer organisations claim to have formal enterprise risk management in place.
• About 70% of organisations would not describe their risk management oversight as mature.
• 40% or fewer organisations are satisfied with the reporting of information about top risk exposures to senior management.
• Less than 30% view their risk management process as providing competitive advantage.

Who could drive positive change?
Who could drive positive change?
Who could drive positive change?
Who could drive positive change?

SENIOR MANAGEMENT
Who could drive positive change?

THE IIA

2120 – Risk Management
“The internal audit activity must evaluate the effectiveness and contribute to the improvement of the risk management process”
Who could drive positive change?

REINVENTING internal audit

Tim J. Leech

Recent governance-related developments require the profession to revisit some of its long-held paradigms.

© Risk Oversight Solutions Inc.
Who could drive positive change?
Who could drive positive change?

“NEVER BELIEVE THAT A FEW CARING PEOPLE CAN’T CHANGE THE WORLD. FOR, INDEED, THAT’S ALL WHO EVER HAVE.”

MARGARET MEAD

© Lifehack Quotes
Barriers to Paradigm Shifts

The greatest barrier to a paradigm shift is the reality and incredible inertia of paradigm paralysis. A paradigm paralysis can be defined as the inability or refusal to see beyond current models of thinking. There are countless examples of paradigm paralysis in the history of mankind. In Europe, up until the XVII century, physicians used to draw out substantial amount of blood from their patients to “purify” their bodies from some imaginary “miasma”. It would, of course, make patients weaker and quicken their death. The first physicians to challenge this absurdity were dismissed and banned from the profession. A better known example of paradigm paralysis is the rejection of Galileo’s theory of a heliocentric universe which revolutionized the field of astronomy.

Source: http://newsjunkiepost.com/2011/09/04/will-we-have-a-global-paradigm-shift-away-from-obsolete-ideologies/
Barriers to change

Regulator paradigm paralysis
Barriers to change
Barriers to change

The Three Lines of Defense Model

Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41
In the absence of real and serious pressure to change, human beings often resist rapid radical change

**Calls for Improved Enterprise-Wide Risk Oversight**

68% indicate that the board of directors is asking “somewhat” to “extensively” for increased senior executive involvement in risk oversight. That is even higher for large companies (86%) and public companies (88%).

- 65% of organizations experience “somewhat” to “extensive” pressure from external parties to provide more information about risks.
- Financial services organizations are especially experiencing these external pressures with 79% experiencing them “somewhat” to “extensively.” These demands are most notably coming from regulators.

**Risk Oversight Leadership**

32% have designated an individual to serve as the chief risk officer or equivalent.

- Financial services organizations are most likely to designate an individual as CRO or equivalent, with such appointments occurring in 56% of the firms surveyed.

45% have a management-level risk committee

- For most organizations with a risk management committee, the committee meets at least quarterly.

Source:
The Way Forward: Objective Centric ERM/IA

FIVE LINES OF ASSURANCE
The Five Lines of Assurance model significantly elevates the role of CEOs and boards of directors in risk governance.

Board of Directors
The Board has overall responsibility for ensuring there are effective risk management processes in place and the other four lines of assurance are effectively managing risk within the organization’s risk appetite and tolerance. The Board also has responsibility for assessing residual risk status on board level objectives (CEO performance and succession planning, strategy, etc.).

Internal Audit
Internal audit provides independent and timely information to the board on the overall reliability of the organization’s risk management processes and the reliability of the consolidated report on residual risk status linked to top value creation and potentially value eroding objectives delivered by the CEO and/or his or her designate.

CEO & C-Suite
CEO has overall responsibility for building and maintaining robust risk management processes and delivering reliable and timely information on the current residual risk status linked to top value creation and potentially value eroding objectives to the board. This includes ensuring objectives are assigned owner/sponsors who have primary responsibility to report on residual risk status. Owner/sponsors often include C-Suite members.

Specialist Units
These groups vary but can include ERM support units, operational risk groups in financial institutions, safety, environment, compliance units, legal, insurance and others. They have primary responsibility for designing and helping maintain the organization’s risk management processes and working to ensure the frameworks and the owner/sponsors of individual objectives produce reliable information on the residual risk status linked to the top value creation and potentially value erosion objectives.

Work Units
Business unit leaders are assigned owner/sponsor responsibility for reporting on residual risk status on objectives not assigned to C-Suite members or other staff groups like IT. These may be sub-sets of top level value creation/strategic objectives and high level potential value erosion objectives.
Objective Centric ERM & Internal Audit: 5 Step Overview

**Step 1**
Populate ‘Objectives Register’ with top value creation and value preservation objectives.

**Step 2**
Assign objective ‘Owner/Sponsors’ and identify ‘Risk Assessment Rigor’ (‘RAR’) and ‘Independent Assurance Level’ (‘IAL’) targets.

**Step 3**
Confirm decisions made in Step 1&2 on Objectives Register, Risk Assessment Rigor and Independent Assurance Levels with the Board.

**Step 4**
Owner/Sponsors complete RiskStatuslines™ and Internal Audit/other assurance groups complete independent assurance work.

**Step 5**
Consolidated report including ‘Composite Residual Risk Ratings’ prepared for senior management and the Board.
The Way Forward: Objective Centric ERM/IA

RiskStatusline™

End Result Objective
(Implicit or Explicit)

Internal/External Context

Threats to Achievement/Risks?

Risk Treatment Strategy
risk mitigators/controls
risk transfer, share, finance
(Selected consciously or unconsciously)

Residual Risk Status

Acceptable?

NO
Re-examine risk treatment strategy and/or objective and develop action plan

YES

Risk Treatment Optimized?

NO

YES – Move On

Statement of an End Result Objective
e.g. customer service, product quality, cost control, revenue maximization, regulatory compliance, fraud prevention, safety, reliable information, and others.

External and Internal Environment
the organisation seeks to achieve its objectives.

Threats to Achievement/Risks are real or possible situations that create uncertainty regarding achievement of the objective.

Risk Treatments manage uncertainty that the objective will be achieved by mitigating, transferring, financing, or sharing risks.

Residual Risk Status is a composite snapshot that helps decision makers assess the acceptability of the retained risk position.

Status data includes performance data, potential impact(s) of not achieving the objective, impediments, and any concerns regarding risk treatments in place. (NOTE: “control deficiencies” are called concerns)

Is the residual risk status acceptable to the work unit? Management? The Board? Other key stakeholders? (i.e. managed within risk appetite/tolerance)

Is this the lowest cost combination of risk treatments given our risk appetite/tolerance?

© 2015 Risk Oversight Solutions Inc.
Polling Question #3
Which of the following groups will likely experience the least difficulty with a move to OCERM/IA:

a) Internal audit because most IA shops already focus on top value creation objectives on all their audits

b) ERM specialists because the majority of ERM practitioners already focus on the top value creation objectives critical to business success

c) Boards because they have been told they should actively oversee strategy, the risk management framework, and risk appetite/tolerance in their organization

d) CEOs because they will welcome more board oversight on top value creation objectives

e) Don’t know
• Boards are active participants, not bystanders.

• Communicates and reinforces the key role the CEO and the Board must/should play in ERM going forward.
OCERM/IA: the business case

• Emphasis is on risk taking and risk treatment

• Senior management and boards are provided with a concise picture of the state of residual risk status linked to the organization’s top value creation and erosion objectives to help them assess its acceptability
OCERM/IA: the business case

- Boards and senior management define the level of risk assessment rigor and independent assurance they want. This defines ERM staff and IA’s scope and resources required.
- Supports better resource allocation decisions.
OCERM/IA: the business case

• The objective is not to minimize risk but rather to optimize the level of risk being accepted to best achieve the organization’s objectives while still operating within an acceptable level of retained/residual risk.

• In addition to analyzing “residual risk status” the process focuses on “optimizing risk treatments” – i.e. the lowest possible cost combination of risk treatments necessary to operate within risk appetite/tolerance
OCERM/IA: the business case

• IA focuses on the top value creation and potential value erosion objectives elevating IA’s stature and value add.

• IA staff must learn to consider and assess the full range of “risk treatments” not just “internal controls”.
• IA actively participates in the process of generating the information necessary for management and boards to assess if the current residual risk status is, or is not, within their risk appetite and tolerance (i.e. per the FSB the “Risk Appetite Framework”)

• IA transitions from the business of providing subjective opinions on “control effectiveness” on a small fraction of the risk universe to ensuring senior management and the board are aware of the current residual risk status linked to key strategic value creation objectives and potential value erosion objectives. Conflict and non-productive haggling over wording, a common problem in direct report internal audit, is reduced significantly
• IA actively participates in the process of optimizing risk treatment design by providing quality assurance reviews and feedback

• IA plays a role ensuring that the board is actively participating in the organization’s strategic planning process and meeting escalating risk oversight expectations

• In organizations with dedicated risk staff their role is to create and maintain the Risk Appetite/risk management framework. IA’s role is to report on the process and reliability of the consolidated report from management on residual risk status
Elevates ERM from what many see as a compliance activity done annually to a key part of strategy development, value creation and better managing potentially value eroding objectives.
The role of ERM support groups is clear – Key role #1 - assist OWNER/SPONSORS of top value creation and potentially value eroding objectives to assess and report on the state of residual risk status to senior management and the board.

The role of ERM support groups is clear – Key role #2 – help OWNER/SPONSORS optimize the risk treatment design (i.e. the lowest cost possible risk treatment design capable of producing an acceptable level of residual risk.
• ERM work better supports the new expectation that boards are responsible for ensuring that effective risk management processes are in place and management is operating the organization within the board’s risk appetite and tolerance.

• The OCERM/IA risk assessment methodology is consistent with ISO 31000 terminology/methodology and provides a solid foundation to meet the principles defined by the Financial Stability Board in their “Principles for an Effective Risk Appetite Framework.”

• ERM support staff receive clear instructions from senior management and the board on the level of risk assessment rigor and independent assurance they want on all objectives in the OBJECTIVES REGISTER.
OCERM/IA: the business case

Risks

Principal Risks, Risk Management and Risk Oversight

The Board is responsible for managing and overseeing risk. A Board-driven, objective centric approach to risk management and internal audit has been adopted that focuses on identifying the most critical value creation objectives and potential value erosion risks if an objective is not met; recording these objectives in a corporate objectives register; assigning specific management personnel in ASVG to objectives to regularly assess and report to the Board on the state of retained/residual risk, including whether the current residual risk status is consistent with the Company’s risk appetite; and direct, senior ASVG management and Board input and involvement in deciding which end-result objectives warrant formal risk assessments; and the appropriate level of risk assessment rigour and independent assurance to be applied in light of cost/benefit considerations. The Board believes this approach better positions the Company to meet the emerging risk governance expectations proposed by the Financial Stability Board (FSB) globally, and the Financial Reporting Council (FRC).

The Companies Act and FRC require companies to disclose the principal risks and uncertainties the Company faces. The Company believes this process is best done by considering the Company’s most important value creation objectives and objectives that have the potential, if not achieved, to significantly erode shareholder value. Independent expert advice has been obtained to ensure that the processes used to populate and maintain the Company’s objectives register and the related residual risk status information are robust, effective, and ‘fit for purpose’.

‘Principal risks and uncertainties’ are defined by the Board as risks with the highest overall potential to affect the achievement of the Company’s business objectives. These objectives include: ensuring the ability to meet liabilities as they fall due and meet liabilities in full; and achieving target returns. Principal risks relating to delivery of these objectives are described on page 30, along with other principal risks identified in relation to other key objectives. Further information on risk factors is set out in note 29 to the Accounts.

Internal control/risk treatment

The Code requires the Board to at least annually conduct a review of the adequacy of the Company’s
OCERM/IA: the business case

THE OCERM/IA TOOLS ARE FREE TO DOWNLOAD
Polling Question #4

Which of the following is **not** one of the strategies recommended in today’s presentation:

a) IA should use management quarterly/annual risk register reports to decide where to do direct report audits and then perform a traditional audit and provide IA’s opinion on internal control effectiveness

b) Use an OBJECTIVE REGISTER as the foundation for all formal assurance work

c) Assign OWNER/SPONSORS to each objective and require they report on residual risk status

d) Require senior management and the board define risk assessment rigour and independent assurance levels for each objective in the OBJECTIVE REGISTER

e) Don’t know
OCERM/IA implementation options

Go Slow Approach #1 – start by doing some audits using RiskStatusline™ method.
Go Slow Approach #2 – run some risk workshops using RiskStatusline™ method
OCERM/IA implementation options

Go Slow Approach #3 – provide orientation to senior management and your board on risk oversight expectations and alternatives to traditional internal audit and ERM methods and seek input
Faster Approach #1 – brief senior management and board on the approach and benefits and seek approval for full implementation over 3-5 years – revolutionary not incremental change
Polling Question #5

Which of the following do you think will pose the greatest barrier to broad adoption of OCERM/IA?:

a) Lack of support for OCERM/IA from IIA global

b) The massive amount of changes that would be required to IIA CIA curriculum and training materials to use a risk assessment process consistent with ISO 31000 and COSO ERM 2017 on all engagements

c) A lack of real interest on the part of CEOs and board members on how IA and ERM specialists do their work

d) Lack of support/active resistance from the risk community for an end result business focus that mandates they quit using risk registers as a foundation for their work

e) All of the above

f) Don’t know
QUESTIONS???

Thank you

timleech@riskoversightsolutions.com