

# *Identifying and assessing risk under ISA 315 (Revised)*

17 SEPTEMBER 2020

PHIL LENTON & JENNY REED

# *Introduction*



Alex Russell  
Technical Manager  
ICAEW

# *Today's presenters*

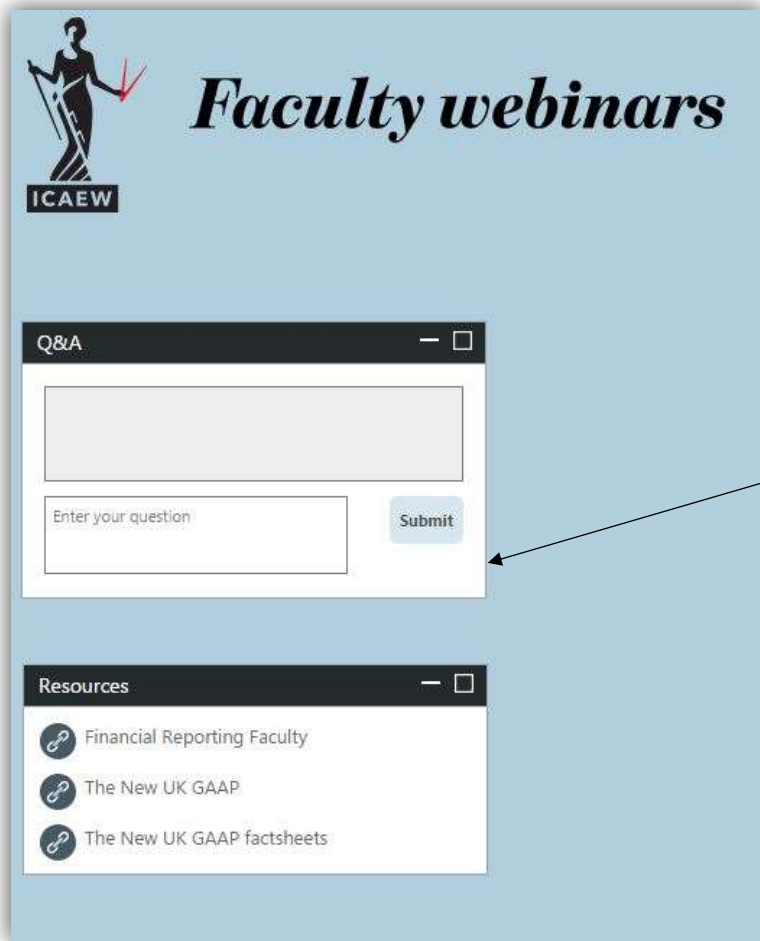


Philip Lenton  
Director  
Deloitte LLP



Jenny Reed  
Global Audit Methodology Manager  
Baker Tilly International

# Ask a question



The screenshot shows the ICAEW Faculty webinars interface. At the top left is the ICAEW logo featuring a figure with a staff and a red ribbon. To the right of the logo is the text "Faculty webinars". Below this is a "Q&A" section with a large text input box and a "Submit" button. Below the "Q&A" section is a "Resources" section with three links: "Financial Reporting Faculty", "The New UK GAAP", and "The New UK GAAP factsheets".



## Audio problems?

- Ensure your volume is turned on
- If you experience poor sound quality try refreshing your page.

## Ask a question

Type your question into the question box then click submit.

[Download resources here](#)

# *Contents*

Overview of the key enhancements

Practical implementation challenges

Specific areas of focus for auditors

Questions



# *Overview of the key enhancements*

## *Application date*

Published by IAASB late December 2019

FRC released ISA (UK) 315 in July 2020 – very minimal UK supplementation

Applies – periods commencing on or after 15 December 2021  
(ie effectively December 2022 year ends)

# *Structure of the new standard*

Number of requirements broadly the same – but **much more granular**

Much more application material (was 156 paragraphs – now 241)

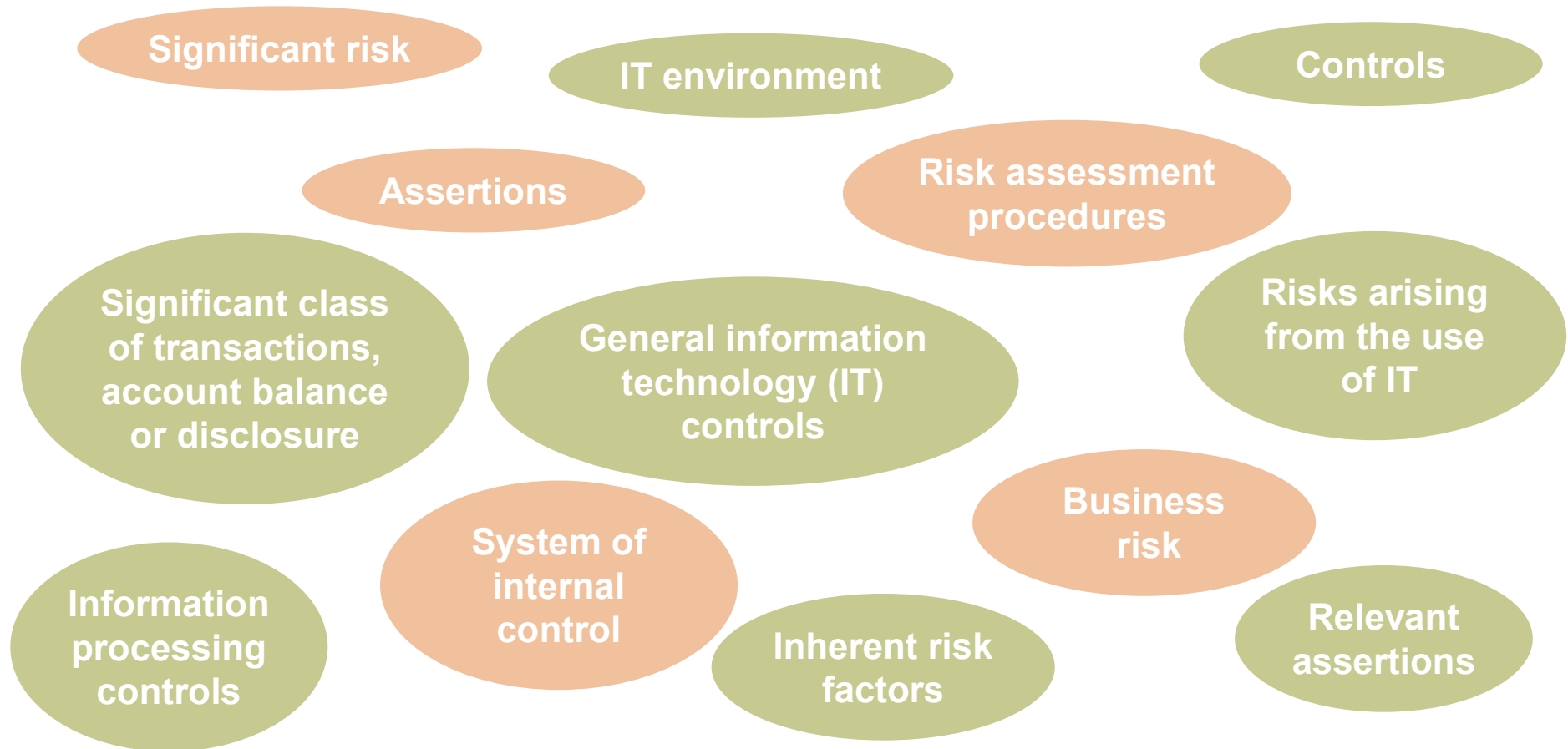
Application material contains a number of examples

6 Appendices with more detailed guidance:

- 1 - Considerations for understanding the entity and its business model
- 2 - Understanding inherent risk factors
- 3 - Understanding the entity's system of internal control
- 4 - Considerations for understanding and entity's internal audit function
- 5 - Considerations for understanding Information Technology (IT)
- 6 - Considerations for understanding General IT Controls



# *New/updated definitions*



# *Inherent and control risk*

Separate assessment of inherent risk and control risk is required

## Inherent risk

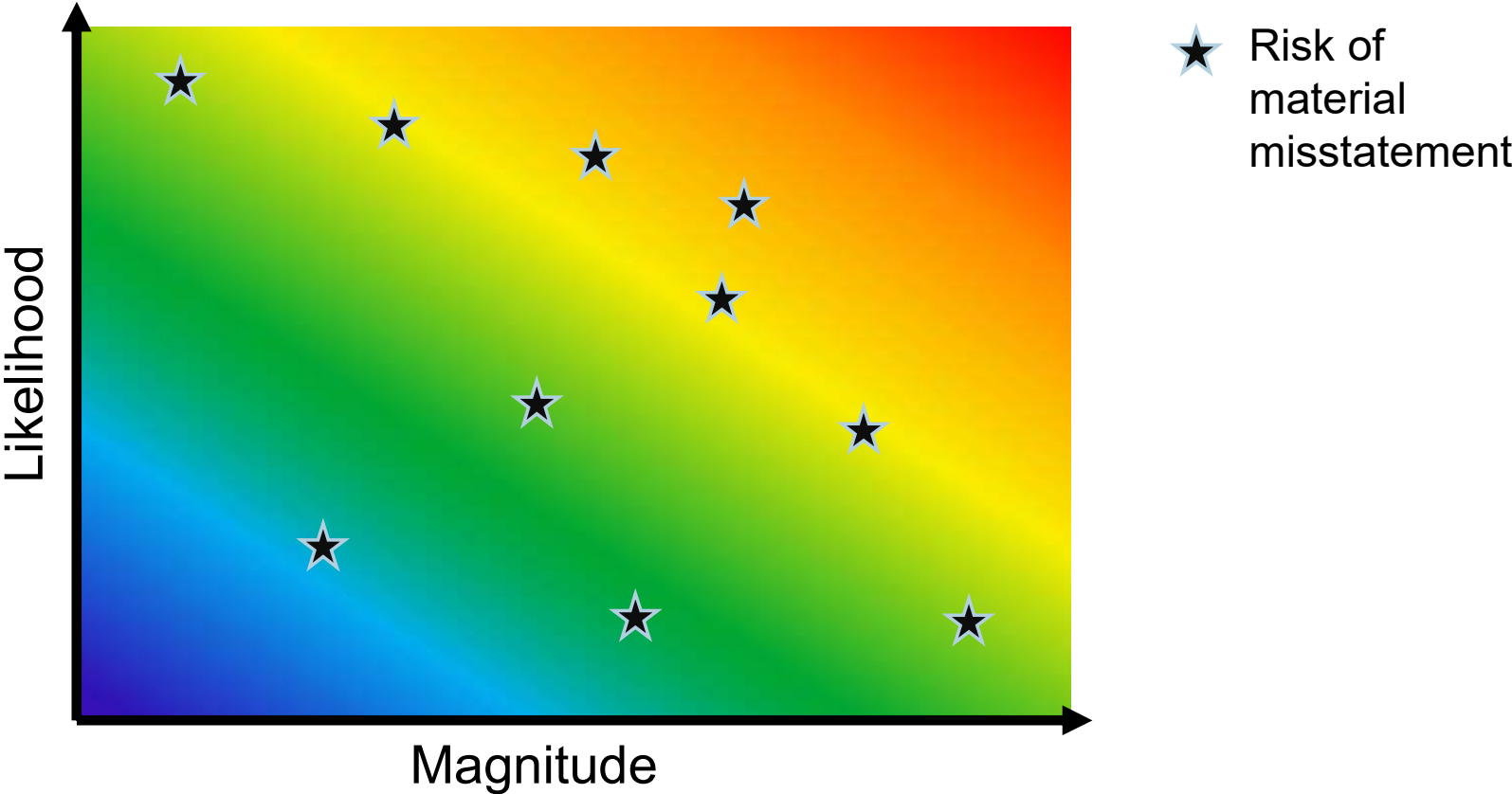
**Susceptibility** of an assertion about a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls

## Control risk

Risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, **will not be prevented, or detected and corrected, on a timely basis by the entity's system of internal control**

Expands this concept from the new ISA 540 to all areas of the audit

# *Spectrum of inherent risk*



# *Spectrum of inherent risk*

Assess inherent risk by assessing the likelihood and magnitude of misstatement

Combination of likelihood and magnitude determines where on the spectrum of inherent risk

Used to design a more precise response to the risk

Varies based on the nature, size and complexity of the entity

Does not mean that both the magnitude and likelihood need to be high

# *Significant risks*

An identified risk of material misstatement:

- For which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur; or
- That is to be treated as a significant risk in accordance with the requirements of other ISAs

In determining significant risks, first identify those assessed risks of material misstatement that have been assessed towards the upper end of the spectrum of inherent risk

Being close to the upper end of the spectrum of inherent risk will differ by entity and period

Depends on the nature and circumstances of the entity

# *Significant risks*

Risks of material misstatement with higher inherent risk and may be significant risks arise from the following:

Transactions for which there are **multiple acceptable accounting treatments** such that **subjectivity** is involved

Accounting estimates that have **high estimation uncertainty or complex models**

**Complexity in data collection and processing** to support account balances

Account balances or quantitative disclosures that involve **complex calculations**

Accounting principles that may be subject to **differing interpretation**

**Changes in the entity's business** that involve changes in accounting, for example, mergers and acquisitions

# *Inherent risk factors*

Complexity

Subjectivity

Change

Uncertainty

Management bias or other  
fraud risk factors

Other events or conditions

Examples of other events or conditions:

- Lack of personnel with appropriate accounting and financial reporting skills
- Control deficiencies in the control environment, risk assessment and monitoring - especially where not addressed by management
- Past misstatements, history of errors or a significant amount of adjustments at period end

# *Control risk*

If plan to test the operating effectiveness of controls, assess control risk

If not plan to test the operating effectiveness of controls, assessment of control risk shall be such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk



# *IT environment and controls*

Clearer delineation between the respective work efforts for understanding the IT environment:

Requirements to obtain an understanding of information processing activities, as part of obtaining the understanding of the information system

Requirements to identify and address risks of material misstatement arising from the use of IT related to the IT applications and other aspects of the IT environment

# *Understanding control activities*

ISA 315 (Revised) brings together all areas the auditor is required to obtain an understanding of control activities:

Controls that address a significant risk

Controls over journal entries

Controls for which the auditor plans to test operative effectiveness


Other controls that the auditor considers are appropriate

# *Understanding IT systems*

Identifying controls that address risks of material misstatement at the assertion level (see previous slide)



Identify the IT applications and the other aspects of the entity's IT environment that are subject to risks arising from the use of IT



Identify:

- i) The related risks arising from the use of IT; and
- ii) The entity's general IT controls that address such risks

# *Strengthened stand back requirement*

Identify significant class of transactions, account balance or disclosure – i.e. where there is one or more relevant assertions

For material classes of transactions, account balances or disclosures that have not been determined to be significant classes of transactions, account balances or disclosures, evaluate whether that determination remains appropriate

Classes of transactions, account balances or disclosures are material if omitting, misstating or obscuring information about them could reasonably be expected to influence the economic decisions of users

# Scalability

Application material incorporates specific considerations and examples to both less and more complex entities

Most sections have specific parts dealing with examples and scalability considerations

## **Example:**

In the audit of many entities, including those with less complex business models and processes, and a less complex information system, the auditor may perform a simple comparison of information, such as the change in interim or monthly account balances from balances in prior periods, to obtain an indication of potentially higher risk areas.

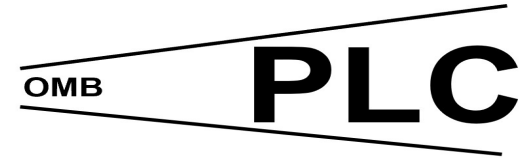
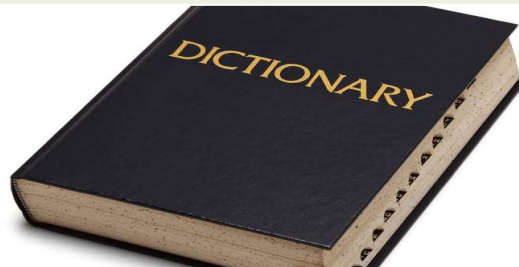
Other entities, typically more complex entities, are expected to have more formalized and documented policies and procedures. The auditor may use such documentation in performing risk assessment procedures.

is of the risk  
the auditor's



# *Practical implementation challenges*

# *Practical implementation challenges: The Standard itself*



Reading the  
revised  
Standard

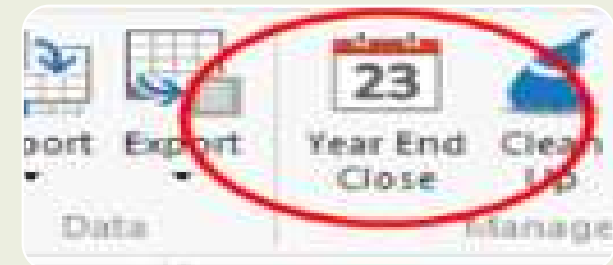
Introductory  
material and  
definitions

Scalability

# *Practical implementation challenges: Methodology changes*



December 2022						
MO	TU	WE	TH	FR	SA	SU
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
						1



New audit  
documentation  
sets

Implementation  
timetable

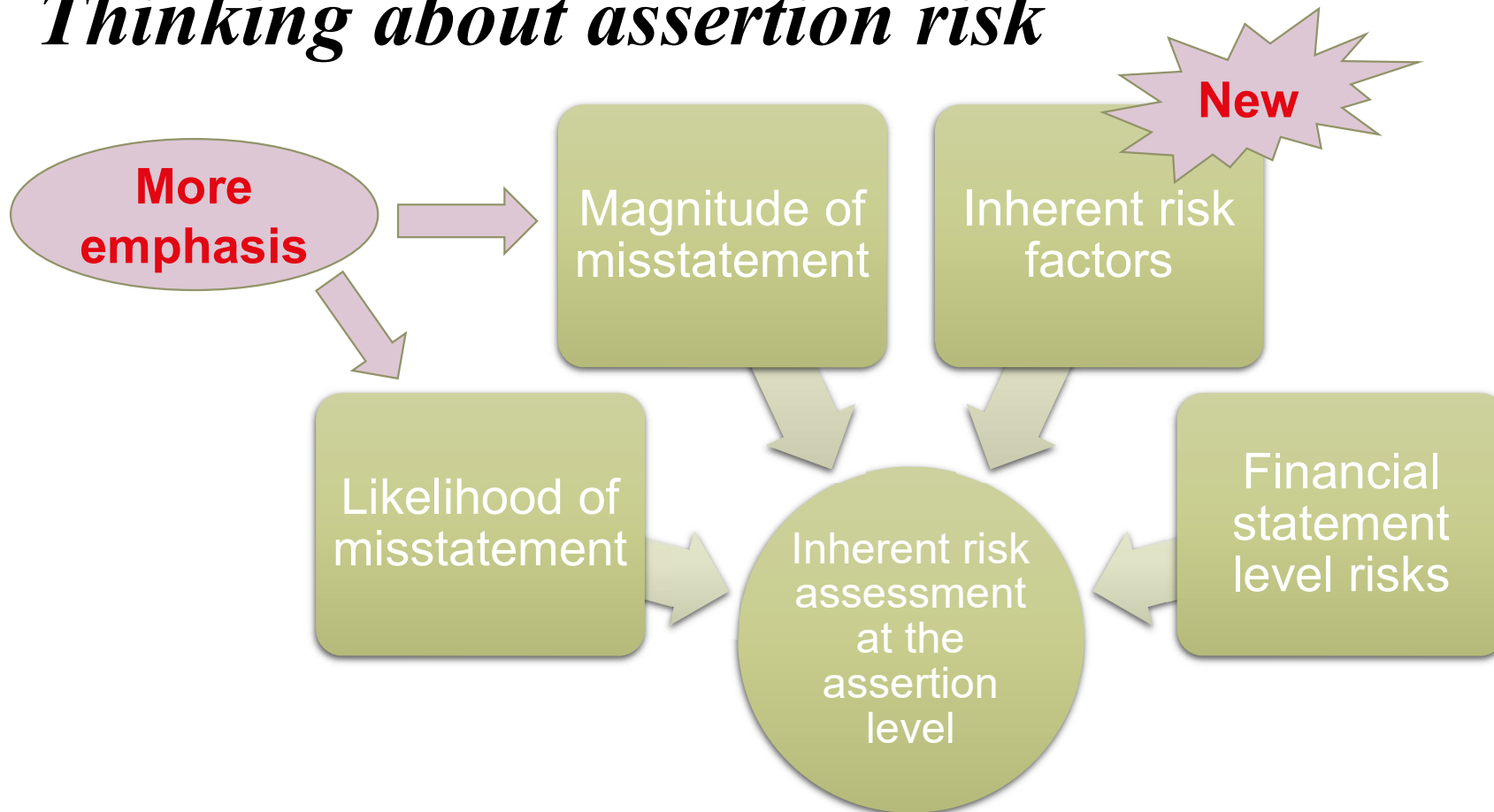
Rolling forward  
prior year files




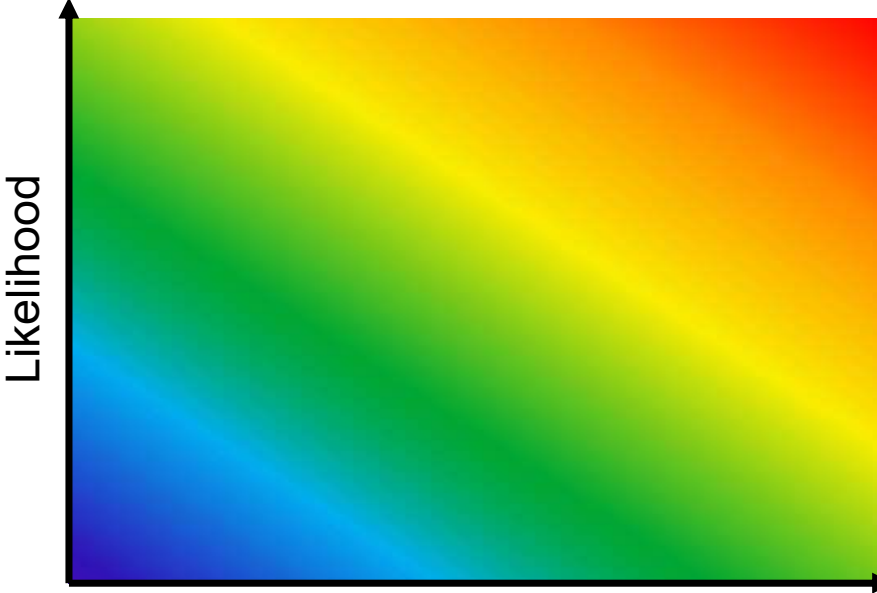


# *Specific areas of focus for auditors*

# *Specific areas of focus for auditors: Thinking about assertion risk*



# *Specific areas of focus for auditors: Spectrum of inherent risk*

Common current approach	ISA 315 (Revised)
 <p>Three identical silver buckets are shown side-by-side. The first bucket on the left has a red letter 'L' on its front, the middle bucket has a red letter 'M', and the right bucket has a red letter 'H'. This represents a discrete, categorical approach to risk assessment.</p>	 <p>A 2D color gradient matrix is shown. The vertical axis is labeled 'Likelihood' and the horizontal axis is labeled 'Magnitude'. The color transitions from dark blue at the bottom-left corner (low likelihood, low magnitude) through green and yellow to red at the top-right corner (high likelihood, high magnitude). This represents a continuous, spectrum-based approach to risk assessment.</p>

# *Specific areas of focus for auditors: Determination of which risks are significant*

## Current approach

Fraud risk

Related to significant economic, accounting  
or other developments

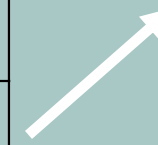
Transaction complexity

Related party involvement

Measurement subjectivity

Outside the normal course of business

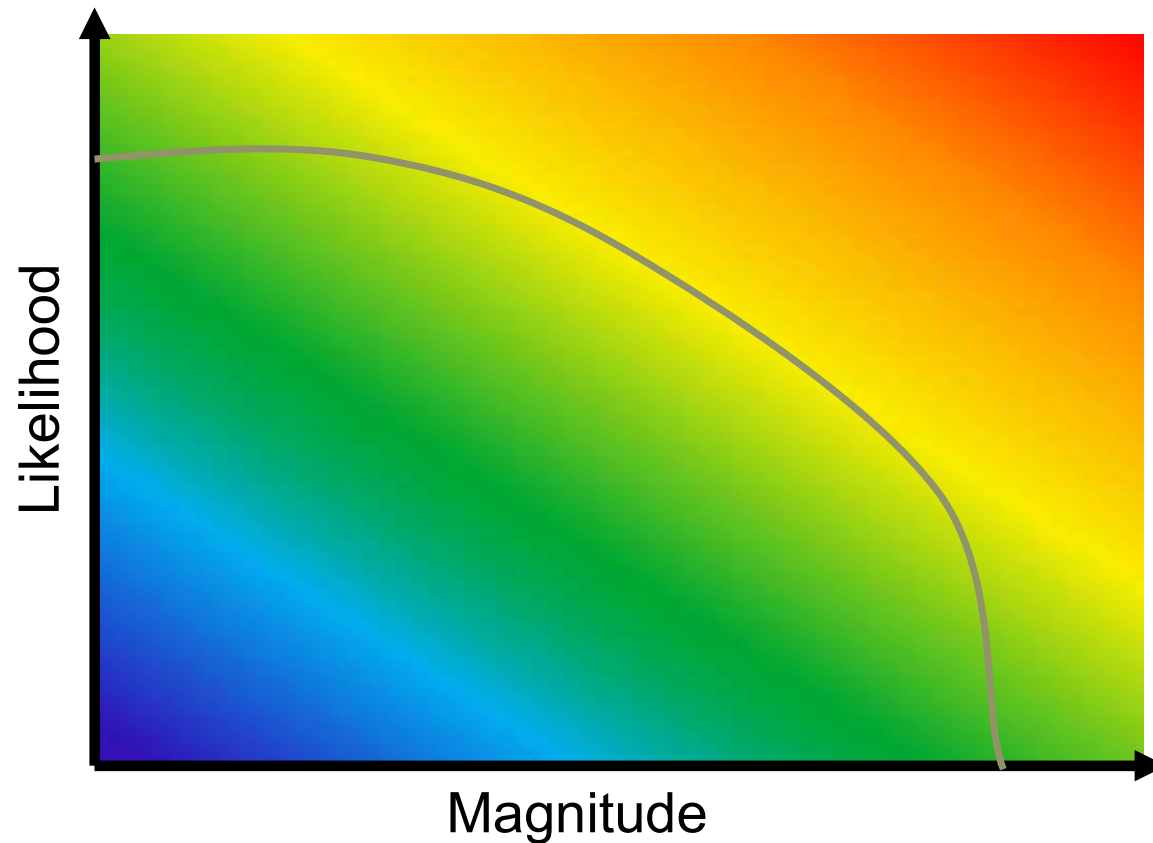
✓
✓



Significant  
risk

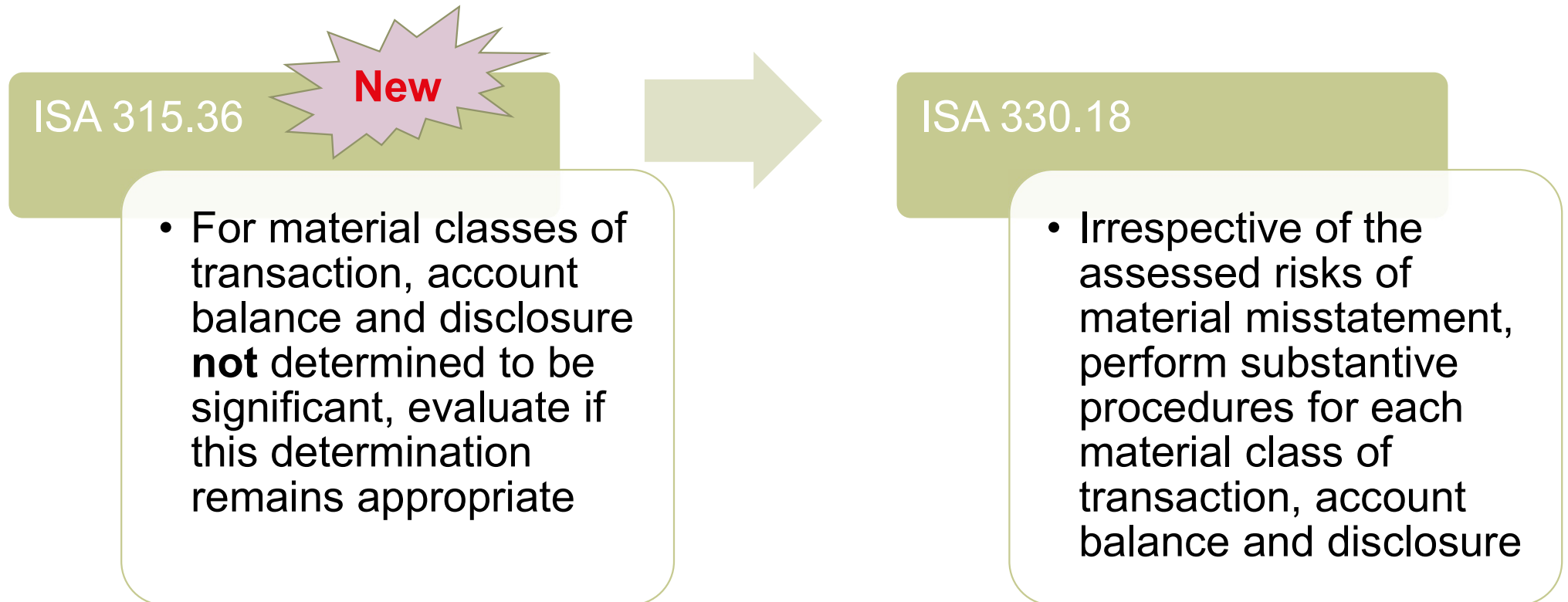
# *Specific areas of focus for auditors: Determination of which risks are significant*

## New approach



- Step 1: Identify risks higher on the spectrum
  - Step 2: Determine which risks are close to the upper end
- ↙ = Significant risks

# *Specific areas of focus for auditors: The “stand back” requirement*



# *Specific areas of focus for auditors: Automated tools and techniques*

Terminology

Examples

Interaction  
with controls

***Specific areas of focus for auditors:  
Controls***

Design and  
implementation  
testing (D&I)

Documentation  
requirements



# *Poll: Areas of greatest difficulty to implement*

Which aspect of ISA 315 (Revised) do you think will be the most difficult to implement?

- a) Risk assessment using the spectrum of inherent risk
- b) Deciding which risks are significant
- c) Understanding IT systems and controls
- d) Scaling the ISA requirements for less complex entities





*Any questions?*

# *Future events*

For details, please visit [icaew.com/aafevents](https://www.icaew.com/aafevents)



14 October – PD Leake Lecture - The art of conversation: the extended audit report

30 October – Going concern and resilience: lessons learned from Covid-19

# *Thank you for attending*



Please take the time to fill out our short survey:  
[Survey link](#)



Contact the Audit and Assurance Faculty

**Phone:** +44 (0)20 7920 8493

**Email:** [tdaf@icaew.com](mailto:tdaf@icaew.com)

**Web:** [icaew.com/AAF](http://icaew.com/AAF)

This webinar is presented by the Audit and Assurance Faculty. Audit and Assurance Faculty membership gives you access to exclusive premium resources including our regular magazine, webinars, discount on events and conferences and extensive online resources to support your career.

For more information about faculty membership and our latest joining offers, please visit [icaew.com/joinaaf](http://icaew.com/joinaaf) or for more information about Faculties Online, please visit [icaew.com/subscribe](http://icaew.com/subscribe).

ICAEW will not be liable for any reliance you place on the information in this presentation. You should seek independent advice.

