ICAEW KNOW-HOW
AUDIT AND ASSURANCE FACULTY

ISA 315: Intelligent auditing, robust assurance

Building the foundations of the exercise of effective professional judgement and scepticism

17 April 2023

Paul Winrow and Rhodri Whitlock

Today's presenters

Dr Paul Winrow
Partner – Head of Audit
and Assurance Methodology
Mazars LLP

Rhodri Whitlock
Director & Founder
HPL Associates Limited -
Audit Quality & Technical Consultancy

Contents

Introduction

ISA 315 – Recap and the ISA ecosystem

Embracing key changes effectively and efficiently

IT and GITC – Demystification and a platform for robust assurance

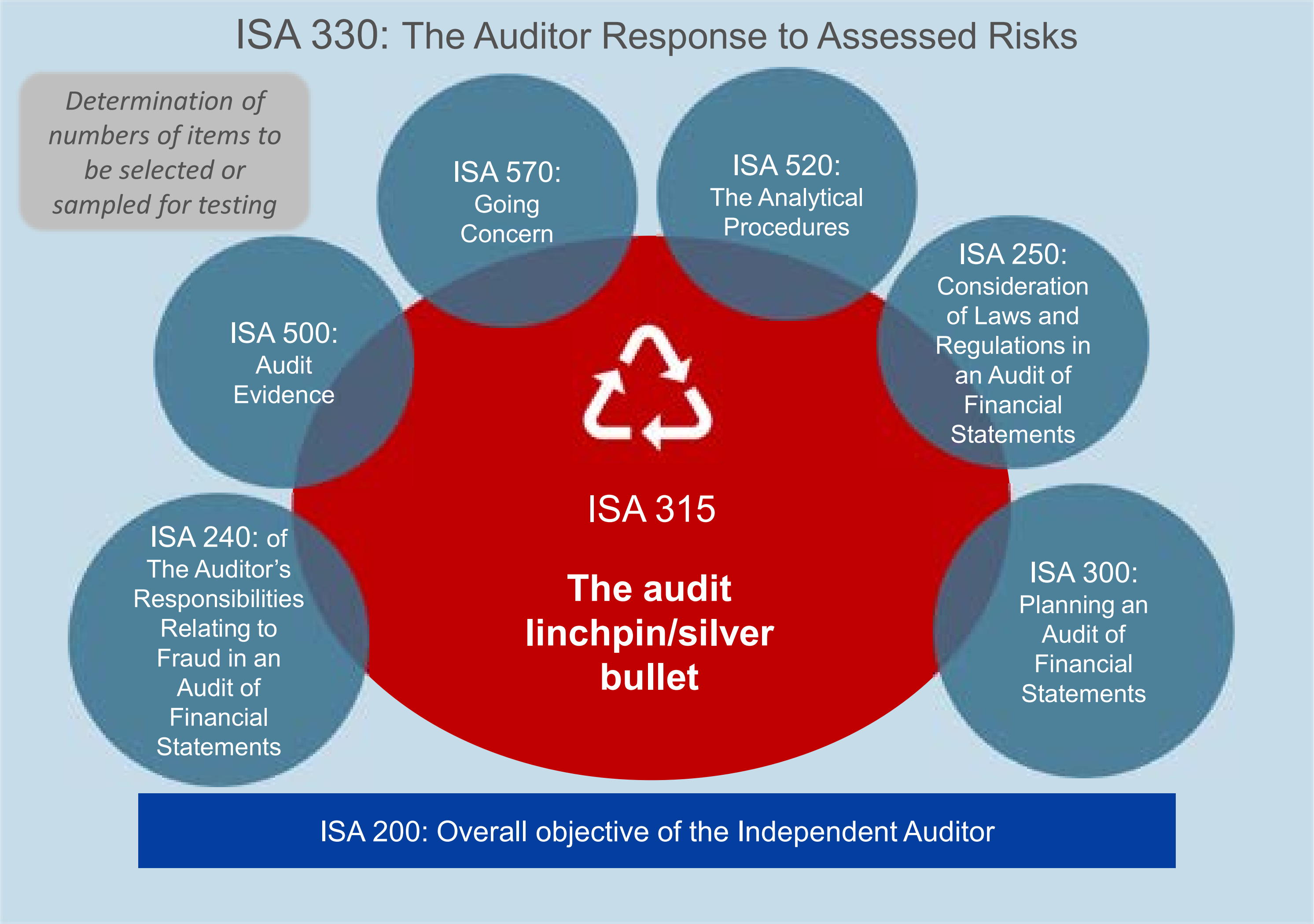
What & How

Summing up

Q&A

ISA 315 – Recap and the ISA ecosystem

Key Context



ISA 330: The Auditor Response to Assessed Risks

Determination of numbers of items to be selected or sampled for testing

ISA 570: Going Concern

ISA 520: The Analytical Procedures

ISA 250: Consideration of Laws and Regulations in an Audit of Financial Statements

ISA 500: Audit Evidence

ISA 315

The audit linchpin/silver bullet

ISA 240: of The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements

ISA 300: Planning an Audit of Financial Statements

ISA 200: Overall objective of the Independent Auditor

Drivers of Change

Formal

Key findings from ISA 315 Implementation Monitoring Project (Completed in 2013)

- Inconsistency over significant risks identified.
- Practical application of obtaining an understanding of the system of internal control.
- Insufficient guidance in respect of IT risks.
- Scalability concerns for SME audits.

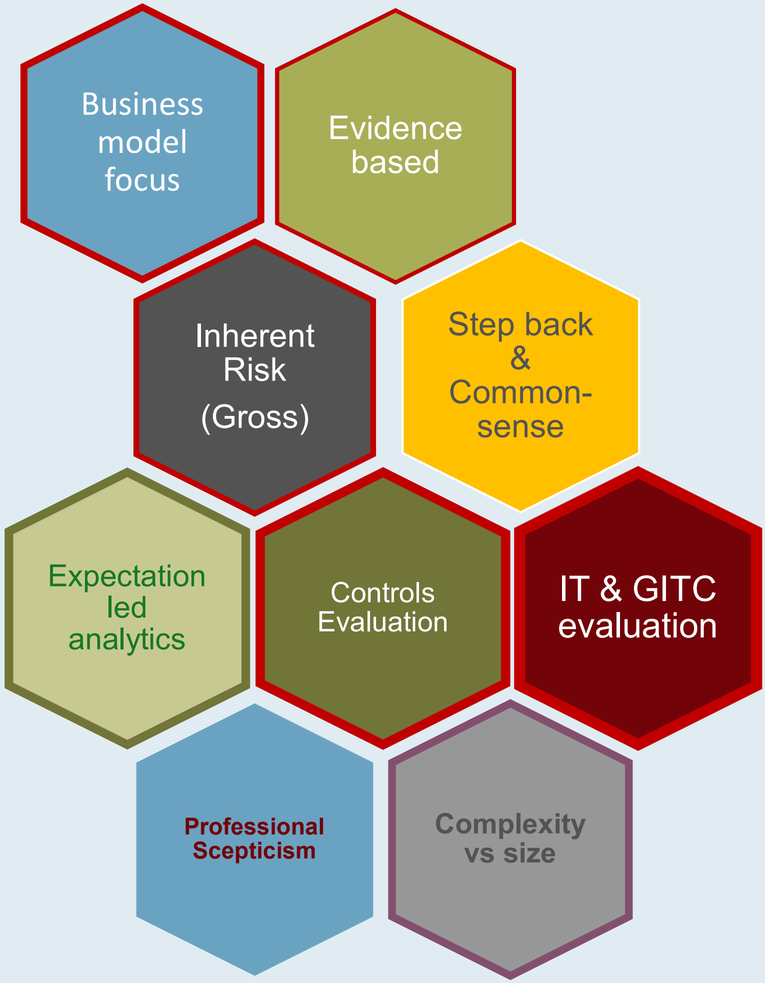
Informal

Consideration of the factors which give rise to poor quality audits (Root Cause Analysis)

- Were audits being built on strong foundations?
- Did the team have the right sector knowledge?
- Reasoned independent expectations vs confirmation bias.
- Insufficient scepticism and challenge?
- Responding to new data and “in-flight” challenges.

Some of the Key Changes

Acting In Public & Stakeholder Best Interests



Business model focus

Evidence based

Inherent Risk (Gross)

Step back & Common-sense

Expectation led analytics

Controls Evaluation

IT & GITC evaluation

Professional Scepticism

Complexity vs size

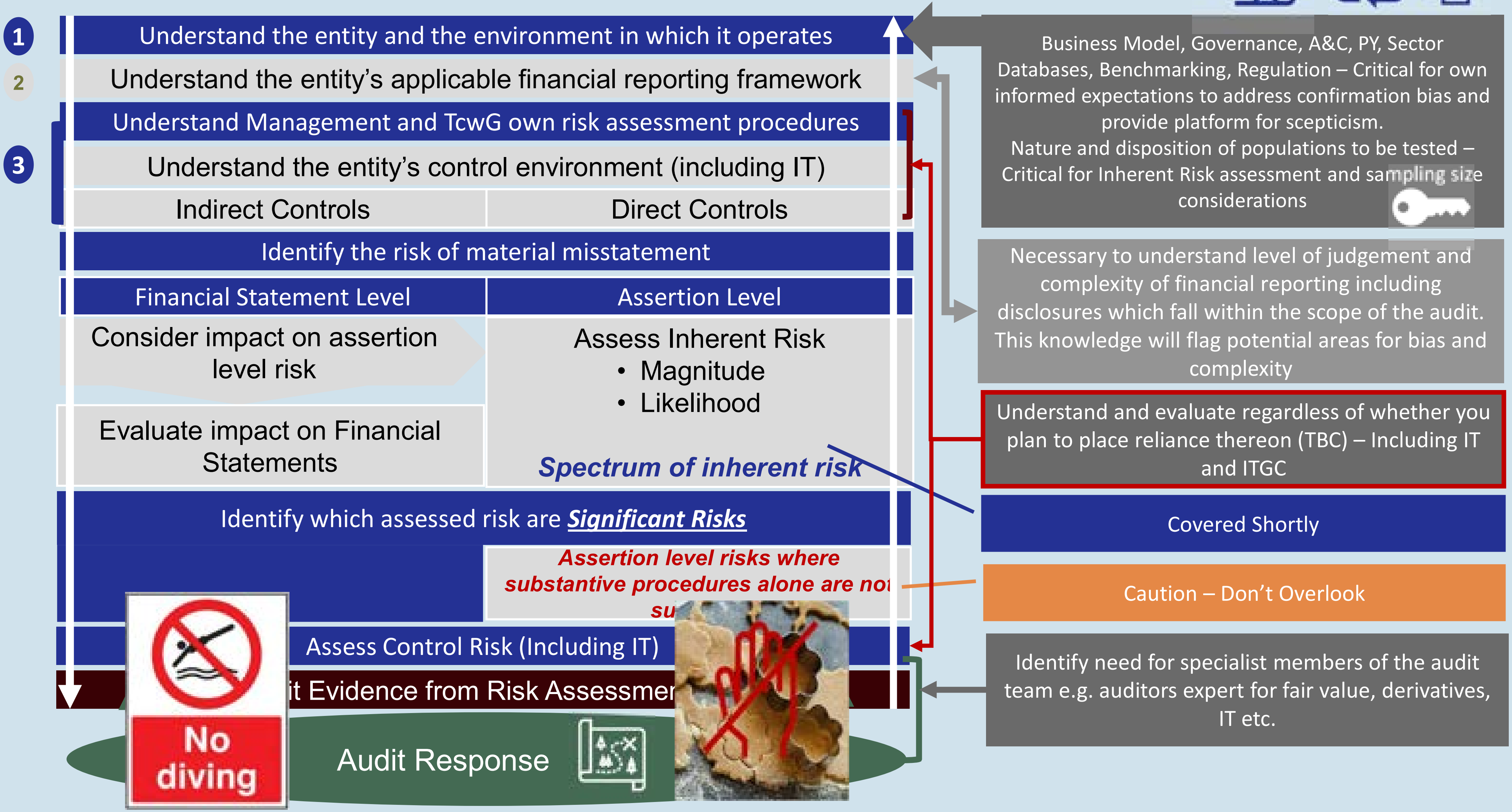
Understand the entity & the environment it operates in

Documentation and Recording of Reasoning is Key – Ticks and clicks not sufficient

Be alert to those areas where substantive testing alone is not enough

Caution, size is not always an indicator of complexity

ISA 315 – A helicopter view



1 Understand the entity and the environment in which it operates

2 Understand the entity's applicable financial reporting framework

Understand Management and TcwG own risk assessment procedures

3 Understand the entity's control environment (including IT)

Indirect Controls | Direct Controls

Identify the risk of material misstatement

Financial Statement Level | Assertion Level

Consider impact on assertion level risk

Evaluate impact on Financial Statements

Assess Inherent Risk
- Magnitude
- Likelihood

Spectrum of inherent risk

Identify which assessed risk are ***Significant Risks***

Assertion level risks where substantive procedures alone are not su

Assess Control Risk (Including IT)

it Evidence from Risk Assessmen

Audit Response

Business Model, Governance, A&C, PY, Sector Databases, Benchmarking, Regulation – Critical for own informed expectations to address confirmation bias and provide platform for scepticism.
Nature and disposition of populations to be tested – Critical for Inherent Risk assessment and sampling size considerations

Necessary to understand level of judgement and complexity of financial reporting including disclosures which fall within the scope of the audit. This knowledge will flag potential areas for bias and complexity

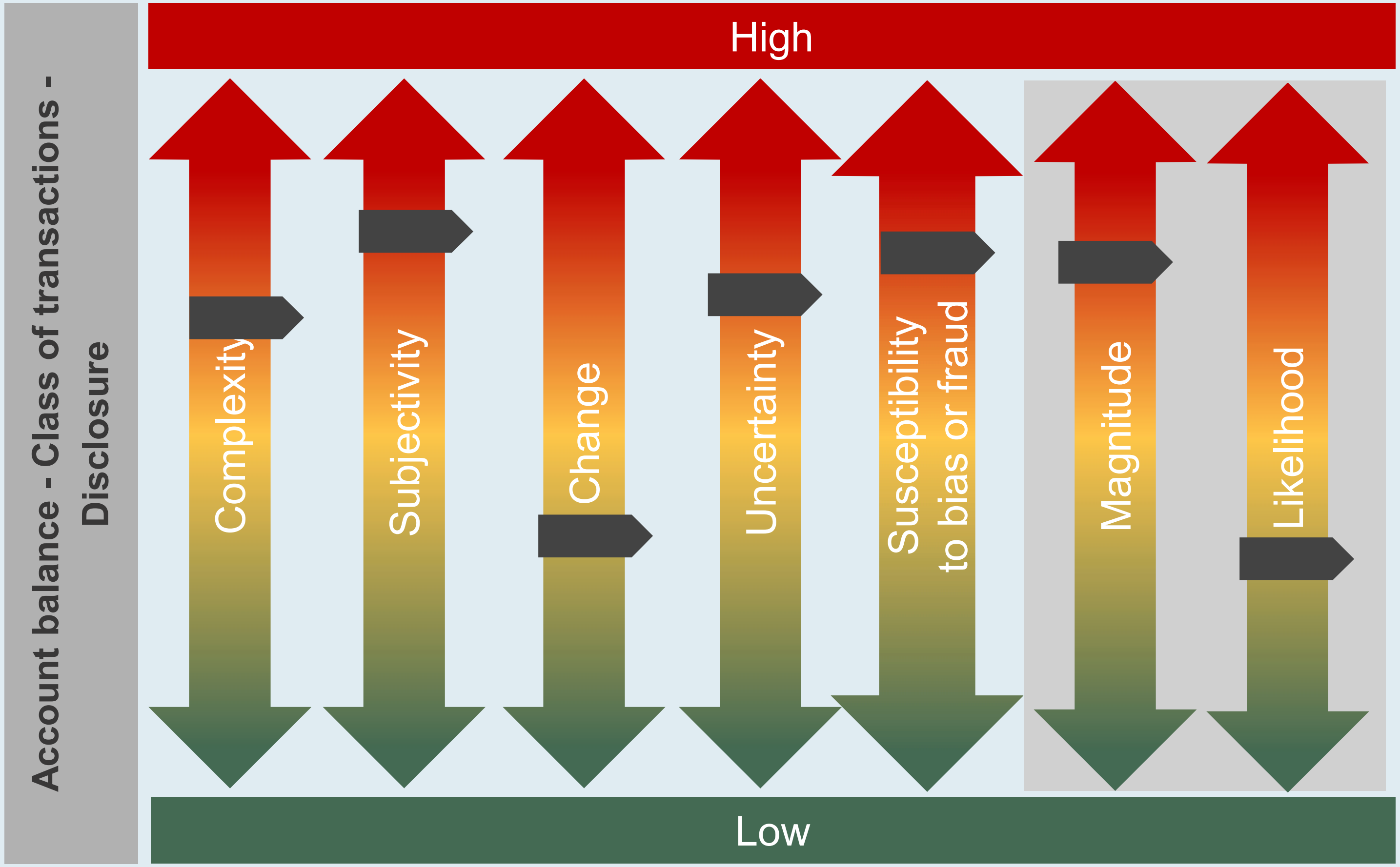
Understand and evaluate regardless of whether you plan to place reliance thereon (TBC) – Including IT and ITGC

Covered Shortly

Caution – Don't Overlook

Identify need for specialist members of the audit team e.g. auditors expert for fair value, derivatives, IT etc.

Assessing Inherent Risk



Account balance - Class of transactions - Disclosure

High

Complexity

Subjectivity

Change

Uncertainty

Susceptibility to bias or fraud

Magnitude

Likelihood

Low

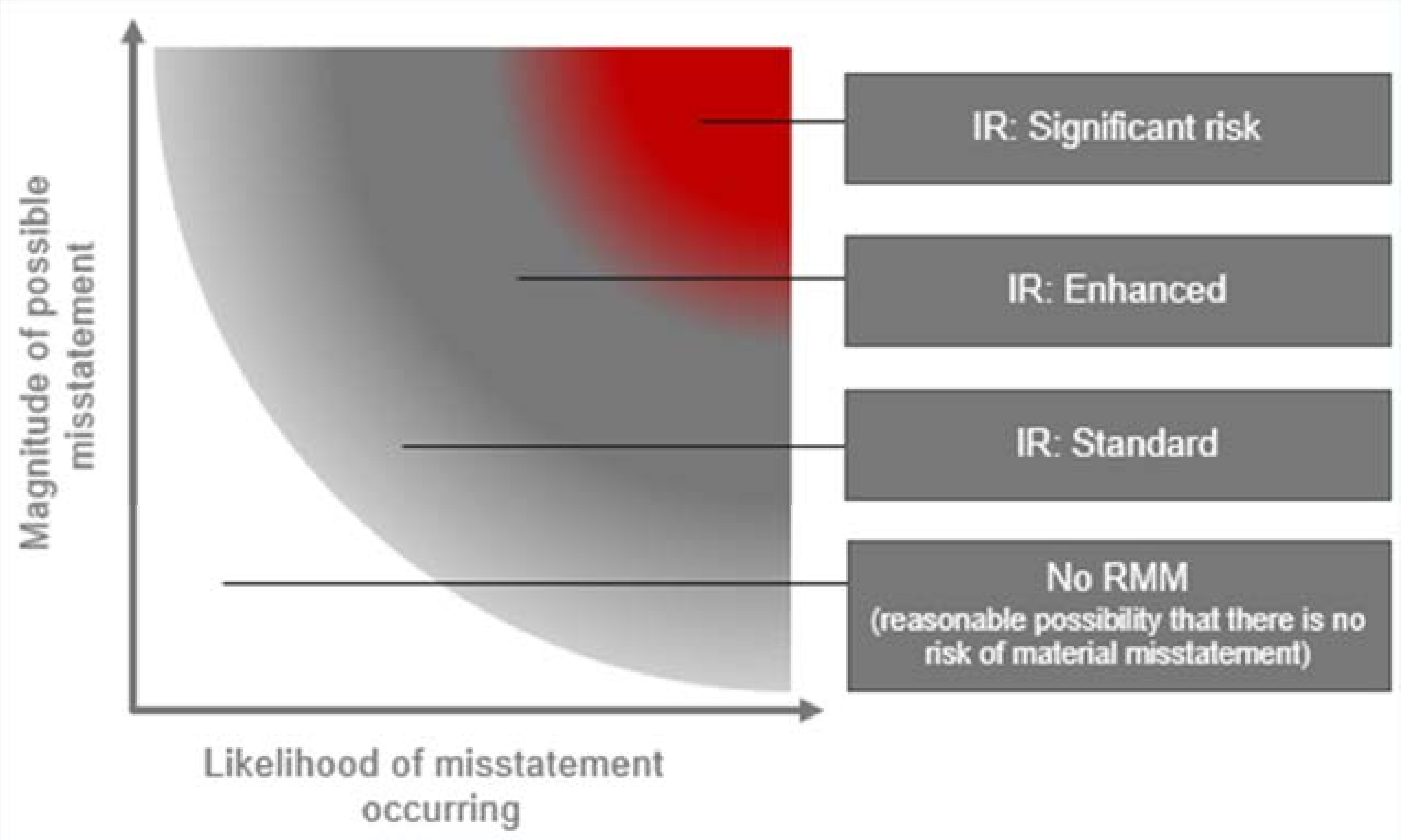
Other Considerations

- Volume
- Uniformity
- Quantitative or qualitative
- Bias Drivers

New Stand-back – Classes of Transactions, Account Balances and Disclosures that are Not Significant but are Material

Evidence, Documentation, Reasoning – Be alert to false negatives from over simplified risk models (more than H,M & L)

Spectrum of Inherent Risk

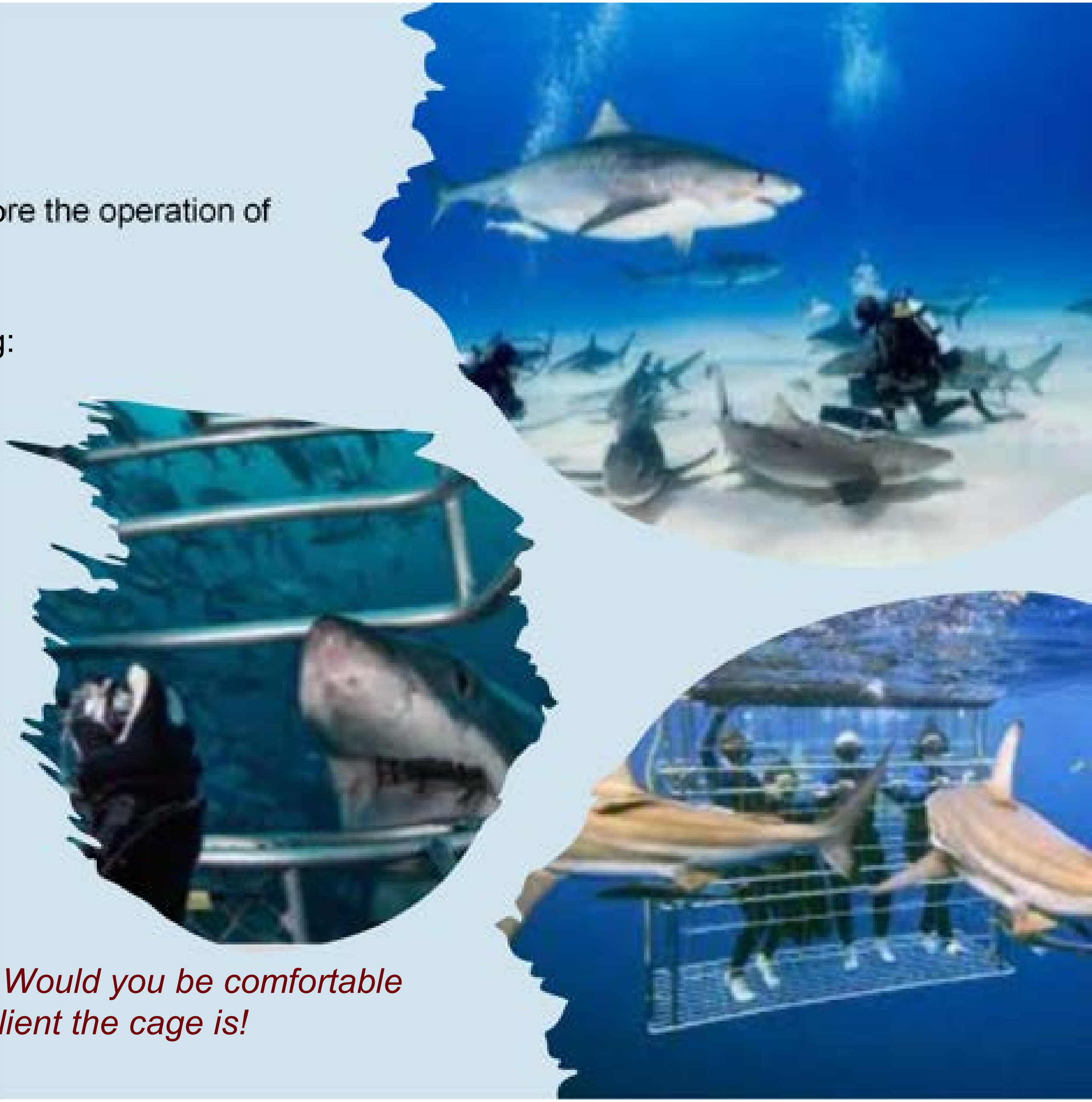

IR: Significant risk
IR: Enhanced
IR: Standard
No RMM
(reasonable possibility that there is no risk of material misstatement)
Magnitude of possible misstatement
Likelihood of misstatement occurring

Inherent (Gross) Risk

Auditors are required to consider inherent risk before the operation of any controls

Not to do so means you are potentially overlooking:

- The true underlying risk of the transaction, account balance or disclosure.
- The need to evaluate and/or test the operation of a key control.
- The identification of a significant risk or KAM.
- The quality and reliability of data you may use during the course of your testing (e.g. substantive analytics).
- The identification of areas where substantive testing on its own may not be sufficient.



Look for and evaluate the control (shark cage). Would you be comfortable signing the audit opinion without know how resilient the cage is!

Embracing key changes effectively and efficiently

So what? – Why the emphasis on the entity and the environment?

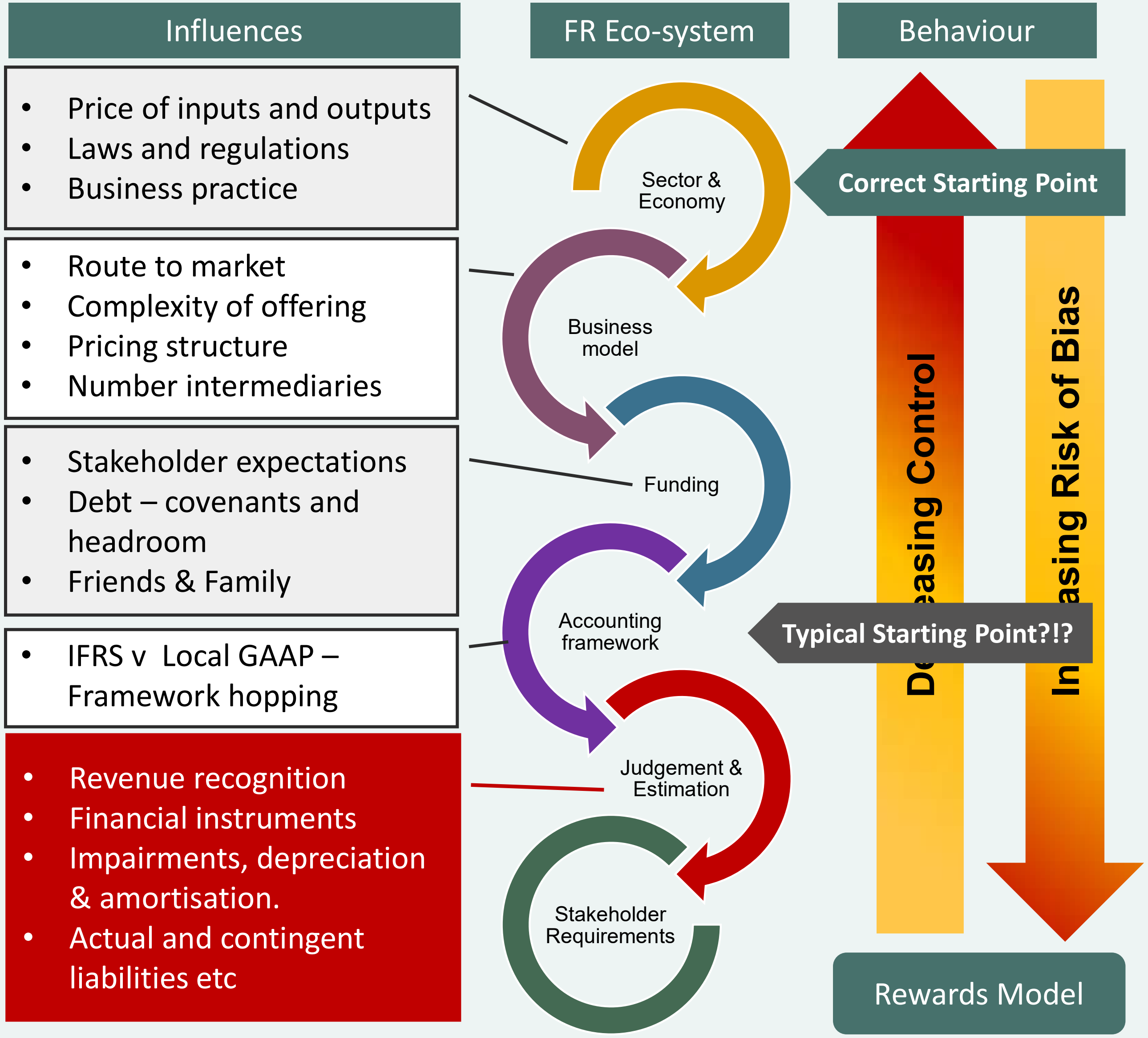
Consider Quality of Earnings or Net Worth

There are many factors which influence quality of earning (or net worth):

This knowledge is key to:

- Independent expectation setting.
- Understanding who are the audit stakeholders
- Effective analytical procedures – throughout all stages of the audit
- Understanding and identification of genuine (not cookie cutter) risks
- Fraud evaluation
- Effective engagement with Management & TCwG
- Selection of materiality benchmark and the appropriate %age
- Designing a truly tailored audit approach

Be objective and look at the whole picture – supports scepticism & constructive informed challenge



Influences

- Price of inputs and outputs
- Laws and regulations
- Business practice

- Route to market
- Complexity of offering
- Pricing structure
- Number intermediaries

- Stakeholder expectations
- Debt – covenants and headroom
- Friends & Family

- IFRS v Local GAAP – Framework hopping

- Revenue recognition
- Financial instruments
- Impairments, depreciation & amortisation.
- Actual and contingent liabilities etc

General Risk Assessment - Procedures and Related Activities: How?

The risk assessment procedures shall include the following:

(a) Inquiries of management and of other appropriate individuals within the entity;

(b) Analytical procedures. (Ref: Para. A27–A31) ;

(c) Observation and inspection. (Ref: Para. A32–A36)

(d) Utilise Information from Other Sources

- Acceptance or continuance procedures.
- Other engagements performed by the engagement partner for the entity. *(checked for relevance and independence considerations).*

(e) Engagement Team Discussion – Not new, but enhanced.

- Proportionate
- More than just a year-on-year comparison
- Business model led
- Sector and company specific intelligence – Benchmarking – Use of derived data – KPIs etc
- Independently informed and targeted expectations
- Cross referrers to ISA 520 for guidance
- The need for informed expectations and the need to be sceptical – avoid the confirmation bias risk

Engage on a ***timely*** basis with Management and Those Charged with Governance

Considerably more than Checklists and Closed Questions

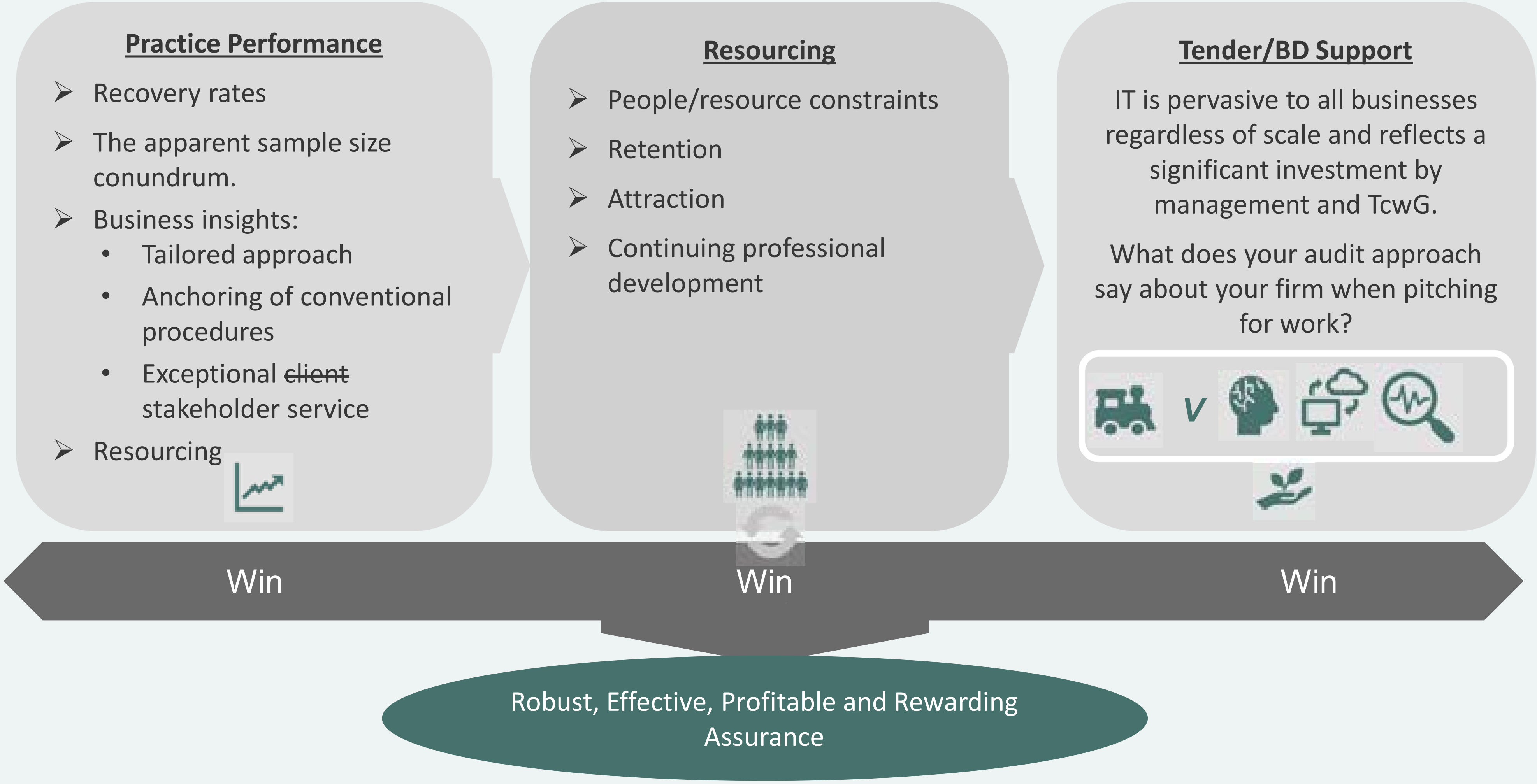
Obtain evidence and document

Don’t undervalue the power of planning analytics it will provide fantastic insights and thought leadership improving the audit and audit relationship

Acknowledgement: FRC ISA 315 Summarised Extract

Controls, IT and GITC Evaluation

“Why bother, we just do substantive testing?” *Why wouldn’t you!*



Practice Performance

- ➢ Recovery rates
- ➢ The apparent sample size conundrum.
- ➢ Business insights:
  - Tailored approach
  - Anchoring of conventional procedures
  - Exceptional ~~client~~ stakeholder service
- ➢ Resourcing

Resourcing

- ➢ People/resource constraints
- ➢ Retention
- ➢ Attraction
- ➢ Continuing professional development

Tender/BD Support

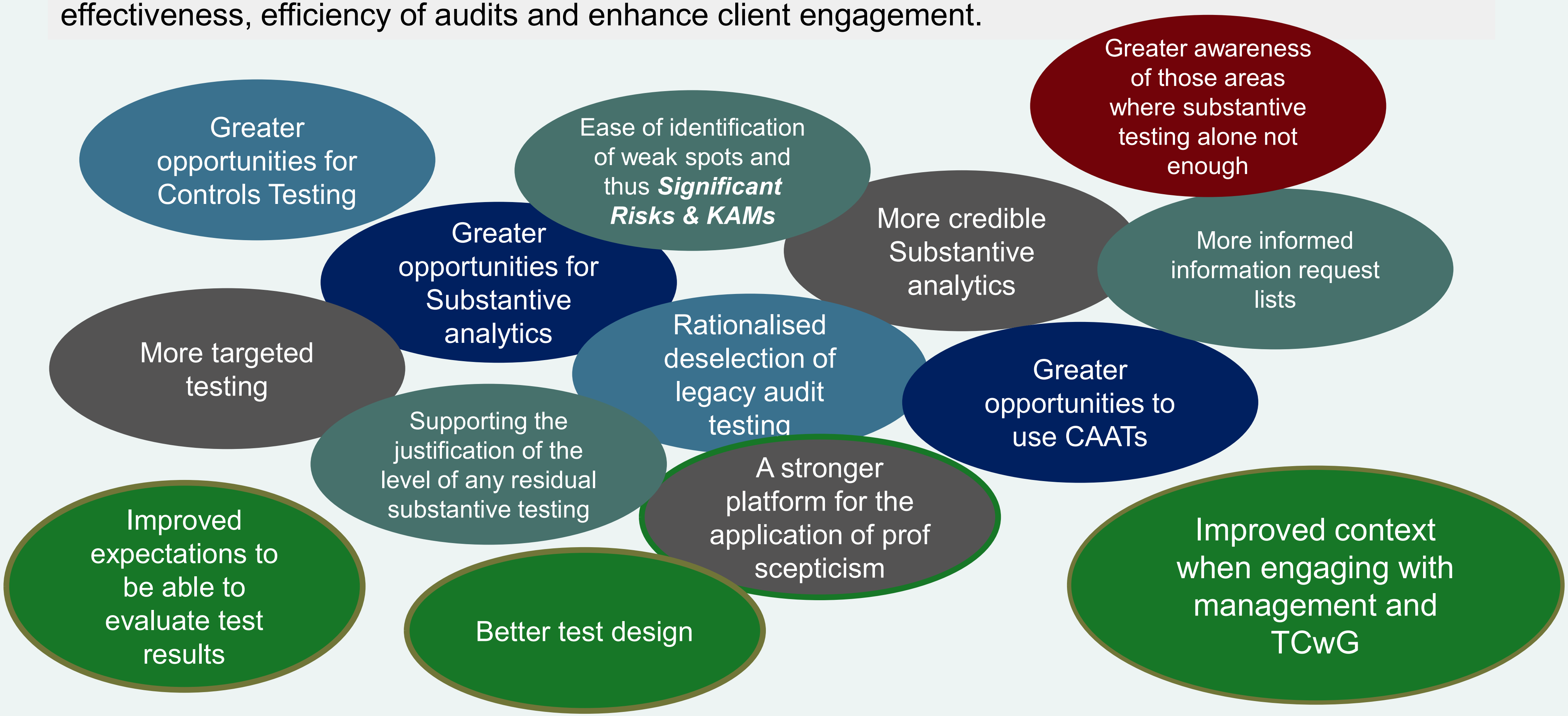
IT is pervasive to all businesses regardless of scale and reflects a significant investment by management and TcwG.

What does your audit approach say about your firm when pitching for work?

Robust, Effective, Profitable and Rewarding Assurance

So, What! What could go right?

In the context of a financial statement audit, the evaluation of controls, IT and GITC can improve the effectiveness, efficiency of audits and enhance client engagement.



Greater opportunities for Controls Testing

Ease of identification of weak spots and thus ***Significant Risks & KAMs***

Greater awareness of those areas where substantive testing alone not enough

Greater opportunities for Substantive analytics

More credible Substantive analytics

More informed information request lists

More targeted testing

Rationalised deselection of legacy audit testing

Greater opportunities to use CAATs

Supporting the justification of the level of any residual substantive testing

A stronger platform for the application of prof scepticism

Improved expectations to be able to evaluate test results

Better test design

Improved context when engaging with management and TCwG

So, What! - What Could Go Wrong?

Account Balances and Transactions

Manipulate prices in sales data bases

Manipulation of spreadsheets - Impairment

Age profile and cash allocation in debtor reports

Manipulate salary rates in HR database

Diversion of sales

Manipulation of spreadsheets – Going Concern

Erroneous or corrupted data download

Diversion of cash

Manipulated spreadsheets - Consolidation

Phantom employees in HR database

Manipulated data transfers – e.g upload TB to Excel ETB

Failure to update standing data

Altering format of automated reporting tools

Manipulated pricing data in stock

Override credit/authorisation limits

KPI and Covenant manipulation

Failure to identify those areas where substantive testing alone may not be enough

GC, NoCLaR & Other Disclosures

Business interruption

Data breaches

Non-compliance with laws and regs

Related Party tracking

Use of unlicensed/ unsupported application

Climate change data

If we don’t evaluate what might go wrong , we will incorrectly evaluate of test results, particularly recognising when there is a need to reassess risk and increase testing

In the context of a financial statement audit, failure to evaluate controls, IT and GITC increases multiple risks and reduces the effectiveness of the audit.

If you still aren’t’ convinced!

ISA 315 say you have to!

Reinforced by:

- ISA 240 - Fraud
- ISA 250 – Laws and Regs
- ISA 500 – Audit Evidence
- ISA 520 – Analytical Procedures
- ISA 570 – Going Concern
- *ISA 260 – Communication with TcwG*
- ***ISA 265 - Communicating Deficiencies in Internal Control to Those Charged With Governance and Management***

Scenario:

Your firm has been engaged as auditor for a few years and you have issued an unqualified opinion and your management letter has been “standard”.

The client makes use of IT across the majority of the elements of its business including sales and HR.

Your audit approach has adopted an “black box approach” on the basis you have “planned” to undertake a substantive audit approach.

You receive a letter from a respected law firm notifying you of a loss your client has suffered due to a payroll and sales rebate “irregularities”.

They should be grateful for your assistance in investigating the matter and would like access to your PY audit file.

INPUT
Black Box
Input is converted into output
OUTPUT

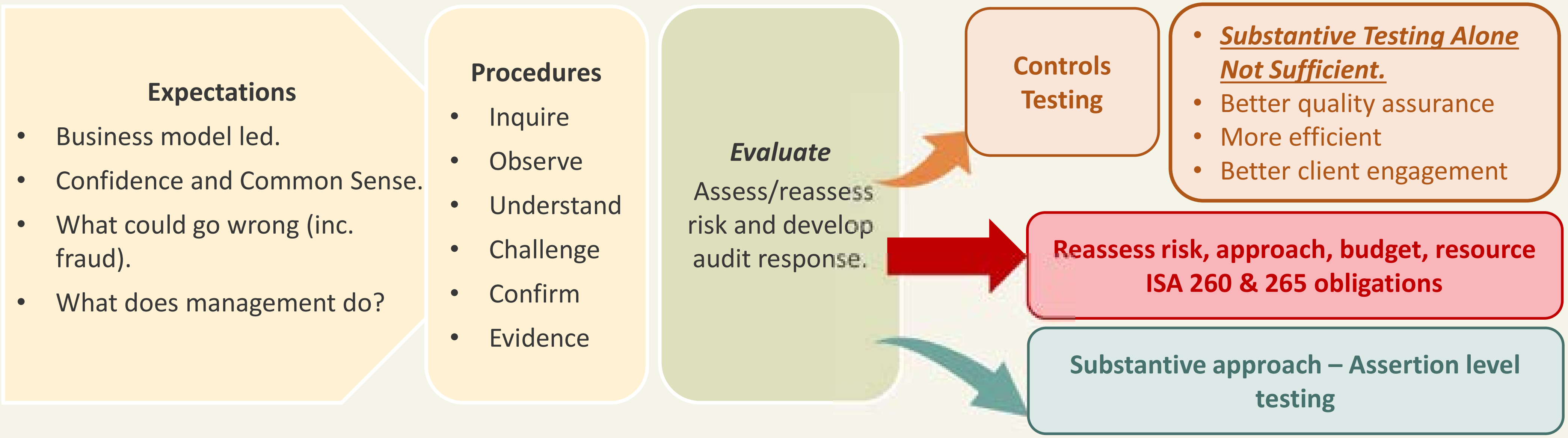
What could go wrong?

Food for thought!

- How do you start to build your defence?
- How do you address management’s assertion that they had not been made aware of the issue and thus deprived of the opportunity to address?

Controls & IT Evaluation Myth Buster

Design & Implementation **Operation & Effectiveness Testing**



Expectations

- Business model led.
- Confidence and Common Sense.
- What could go wrong (inc. fraud).
- What does management do?

Procedures

- Inquire
- Observe
- Understand
- Challenge
- Confirm
- Evidence

Evaluate

Assess/reassess risk and develop audit response.

Controls Testing

- ***Substantive Testing Alone Not Sufficient.***
- Better quality assurance
- More efficient
- Better client engagement

Reassess risk, approach, budget, resource ISA 260 & 265 obligations

Substantive approach – Assertion level testing

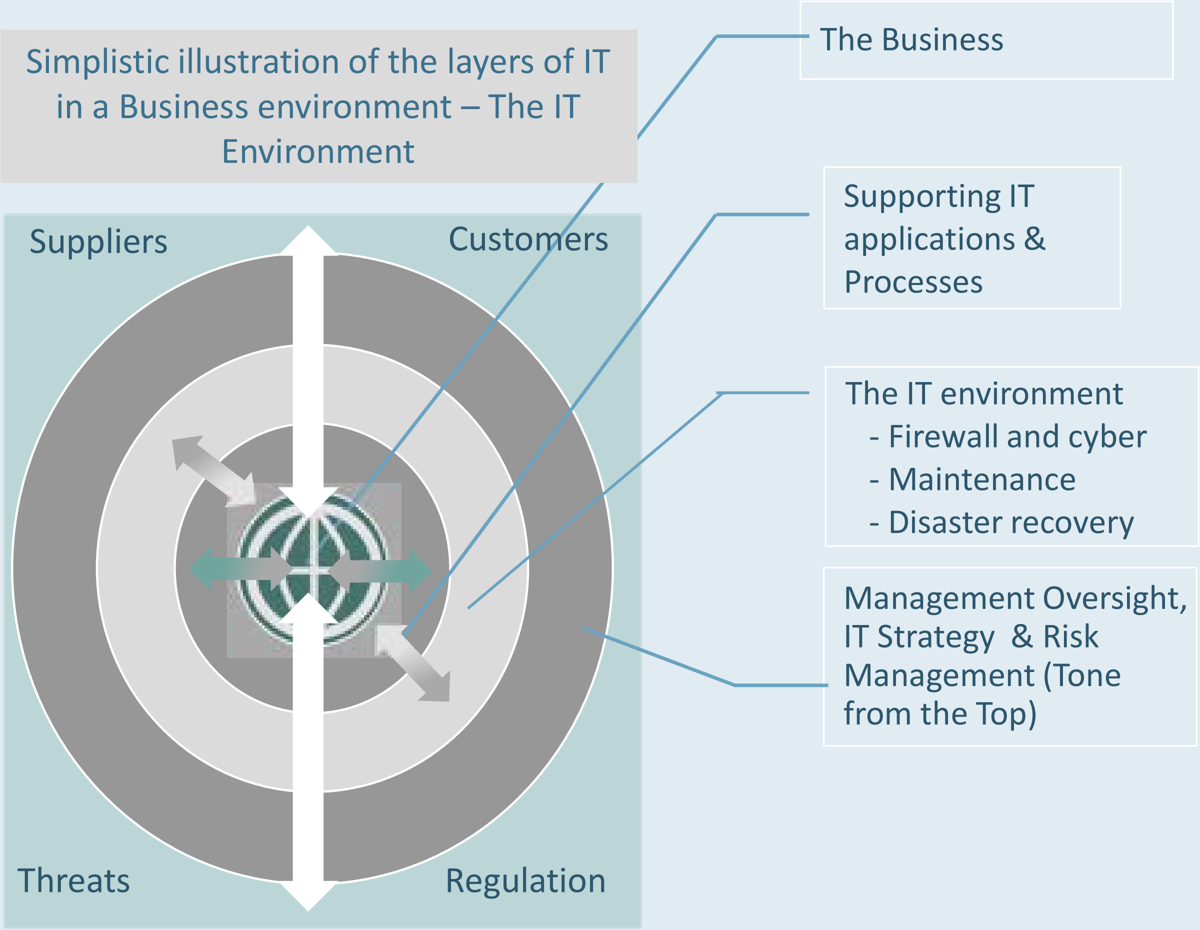
Demystifying IT & GITC

Demystifying the IT environment

Key Considerations

- ***<u>IT is not something separate, it is part of the Business Model.</u>***
- IT is not just about the Tech. Often there are manual controls (e.g. GITC such as access approval).
- Watch out for Spreadsheets and other reporting tools (*<u>User defined application</u>*).
- The ISA is scalable and proportionate.
- Appendices 5 and 6 of ISA 315 are helpful.
- We can all draw on our own everyday experiences of using IT.

Simplistic illustration of the layers of IT in a Business environment – The IT Environment



The Business

Supporting IT applications & Processes

The IT environment
- Firewall and cyber
- Maintenance
- Disaster recovery

Management Oversight, IT Strategy & Risk Management (Tone from the Top)

IT infrastructure - comprises the network, operating systems, and databases and their related hardware and software.

IT application - a program or a set of programs that is used in the initiation, processing, recording and reporting of transactions or information. IT applications include data warehouses and report writers

Proportionality

	Examples of typical environments		
	Non-complex commercial Software	Mid-size and moderately complex commercial software or IT applications	Large or complex IT applications (e.g. ERP systems)
Extent of automation & Use of data	• Simple • Manual inputs • No interfaces • Low data volumes • Local data	• Simple • Small number of inputs and interfaces • Low data volumes or medium volumes of simple data • Local data	• Extensive & complex • Highly automated & multiple interfaces • Large and complex data sets
Type of application and infrastructure	• Purchased off the shelf • Outsourced/cloud • No emerging tech	• Purchased off the shelf or simple low end ERP • Limited customisation • Outsourced/cloud • Limited emerging tech	• Complex • Customised • Large infrastructure • Web-facing • Mixed use of emerging tech
IT Processes	• Simple • Small teams • No source code • Few or no changes • Vendor led updates	Increasing team size and complexity	Very Complex

May not need an IT specialist

Greater likelihood of needing to involve an IT specialist

The greater the volume of data and complexity of the system, be alert to those instances where substantive testing alone may not be sufficient.

- Not just about IT - Can include manual processes and controls.
- Key is understanding how data originates and flows through to the financial statements.
- Understand what could go wrong

Non-complex does not mean you don't need to follow ISA 315 and default to a black box substantive- based approach.

Acknowledgement: FRC ISA 315 Extract and simplification

Typical GITCs

The nature of the general IT controls typically implemented for each of the aspects of the IT environment:

Application Controls

Will correlate to the nature and extent of application functionality and the access paths allowed in the technology. For example, more controls will be relevant for highly-integrated IT applications with complex security options than a legacy IT application supporting a small number of account balances with access methods only through transactions.

Database Controls

Typically address risks arising from the use of IT related to unauthorized updates to financial reporting information in the database through direct database access or execution of a script or program.

Operating System Controls

Typically address risks arising from the use of IT related to administrative access, which can facilitate the override of other controls. This includes actions such as compromising other user's credentials, adding new, unauthorized users, loading malware or executing scripts or other unauthorized programs.

Network Controls

Seek to address risks arising from the use of IT related to network segmentation, remote access, and authentication. Network controls may be relevant when an entity has web-facing applications used in financial reporting. Network controls are also may be relevant when the entity has significant business partner relationships or third-party outsourcing, which may increase data transmissions and the need for remote access.

Inquire – Observe – Understand – Challenge – Confirm – Evidence
Tailor to be relevant of a Financial Statement Audit

- Relevant to all businesses
- Scalable
- Less observable in small non-complex OMB
- Challenges of SaaS

What happens at your firm – how do you access your network and Apps?

What & How

What Controls, IT and GITC do you need to evaluate regardless of a purely substantive audit?

The overall Control and IT "*Environment*" - Holistic

Required Design & Implementation Evaluation (D&I) – Assertion level (mostly)

Controls and IT applications and procedures that relate to:

(i) Identified significant risks;

(ii) Journal entries;

(iii) Those that the auditor plans to test operating effectiveness in determining the nature, timing and extent of substantive testing (***e.g. those risk areas where for which substantive procedures alone do not provide sufficient appropriate audit evidence***);

(iv) Identified fraud risks; and,

(v) Those which in the auditor's professional judgement should be tested to meet the requirements of ISA 330.

Not a Controls and IT resilience audit.

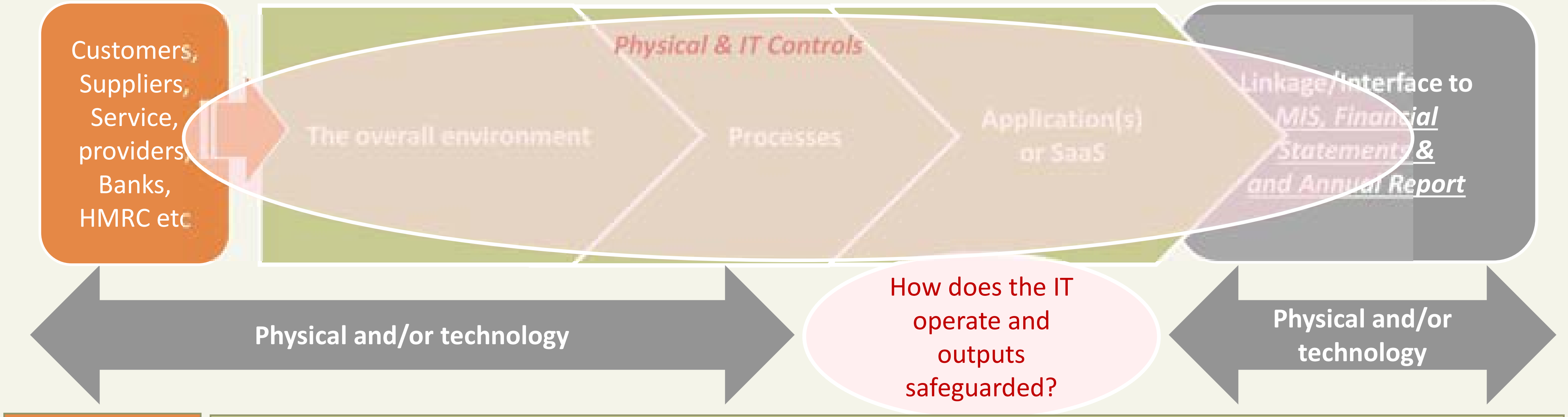
Not a hackathon or disaster recovery test!

Focused on the assertion level risks that are relevant to a financial statement audit.

Not just about IT – Manual Process and Controls may form part of the IT environment

Not as daunting as it may seem as there is a lot of common sense and every day experience we can all draw on.

What! – Where do we start and what is covered?



Customers, Suppliers, Service, providers, Banks, HMRC etc

Physical & IT Controls

The overall environment

Processes

Application(s) or SaaS

Linkage/Interface to *MIS, Financial Statements & and Annual Report*

How does the IT operate and outputs safeguarded?

Physical and/or technology

Physical and/or technology

Potentially daunting?

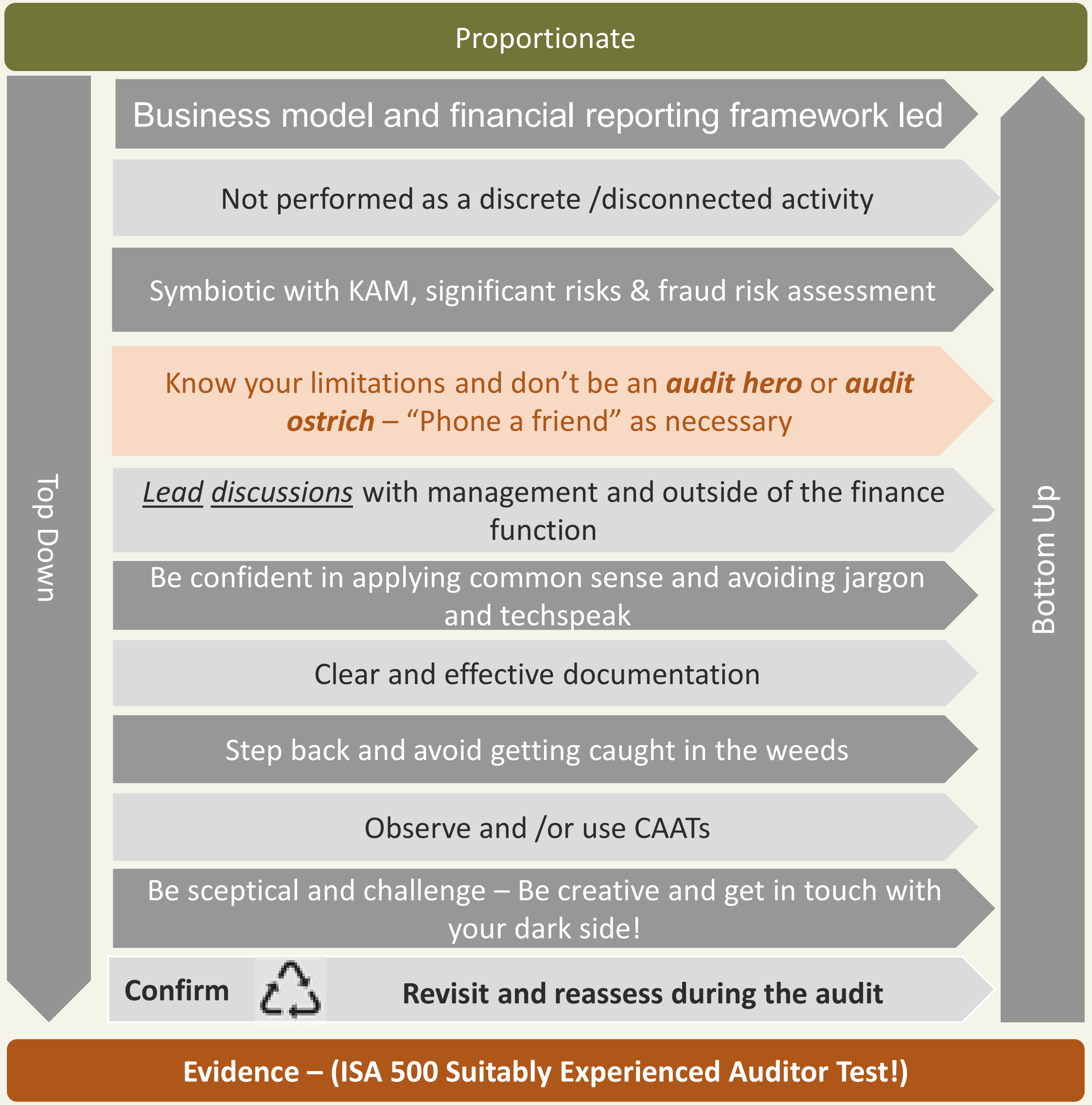
But….We all have plenty of experience and common sense to draw on for most scenarios: Logging in to our practice network, online banking, online shopping, managing our online data and profile, TFA etc Nuclear

Don't get blind sided by jargon and techspeak. Keep it simple:

- What is the origin of each £1 in the annual report, where did it come from;
- How did it get there;
- What (could have) happened to it on the way;
- How was its journey safeguarded; and,
- Don't be seduced by the "simplicity" of spreadsheets and similar.

Watch out for "end user application"
(e.g. Spreadsheets – GC, FV, Impairment, Consolidation, Options …a[illegible]ion of the financi[illegible]s)

How? Understand – Inquire - Observe - Challenge- Confirm - Evidence



Proportionate

Top Down

Business model and financial reporting framework led

Not performed as a discrete /disconnected activity

Symbiotic with KAM, significant risks & fraud risk assessment

Know your limitations and don't be an ***audit hero*** or ***audit ostrich*** – "Phone a friend" as necessary

Lead discussions with management and outside of the finance function

Be confident in applying common sense and avoiding jargon and techspeak

Clear and effective documentation

Step back and avoid getting caught in the weeds

Observe and /or use CAATs

Be sceptical and challenge – Be creative and get in touch with your dark side!

Confirm ♲ **Revisit and reassess during the audit**

Bottom Up

Evidence – (ISA 500 Suitably Experienced Auditor Test!)

Follow the money – from source to the financial statements and in the context of the entity and the environment it operates.

Transactions – Balances – Disclosures including Going Concern & NoCLaR!

Forms expectations to promote scepticism and challenge and reduce confirmation bias and a strong platform for a discussion with management.

Alert to areas where substantive procedures alone may not be sufficient

Effective two way communication with management key. Discussion best and supports the opportunity for scepticism, challenge and strong understanding.

"*A picture paints a 1,000 words*"…Flowcharts are strongly recommended.

Allows information to be quickly digested, key relationships established and highlights weak spots.

Supports "understanding", "Challenge" and "Confirmation"

Facilitates the design of an effective audit response

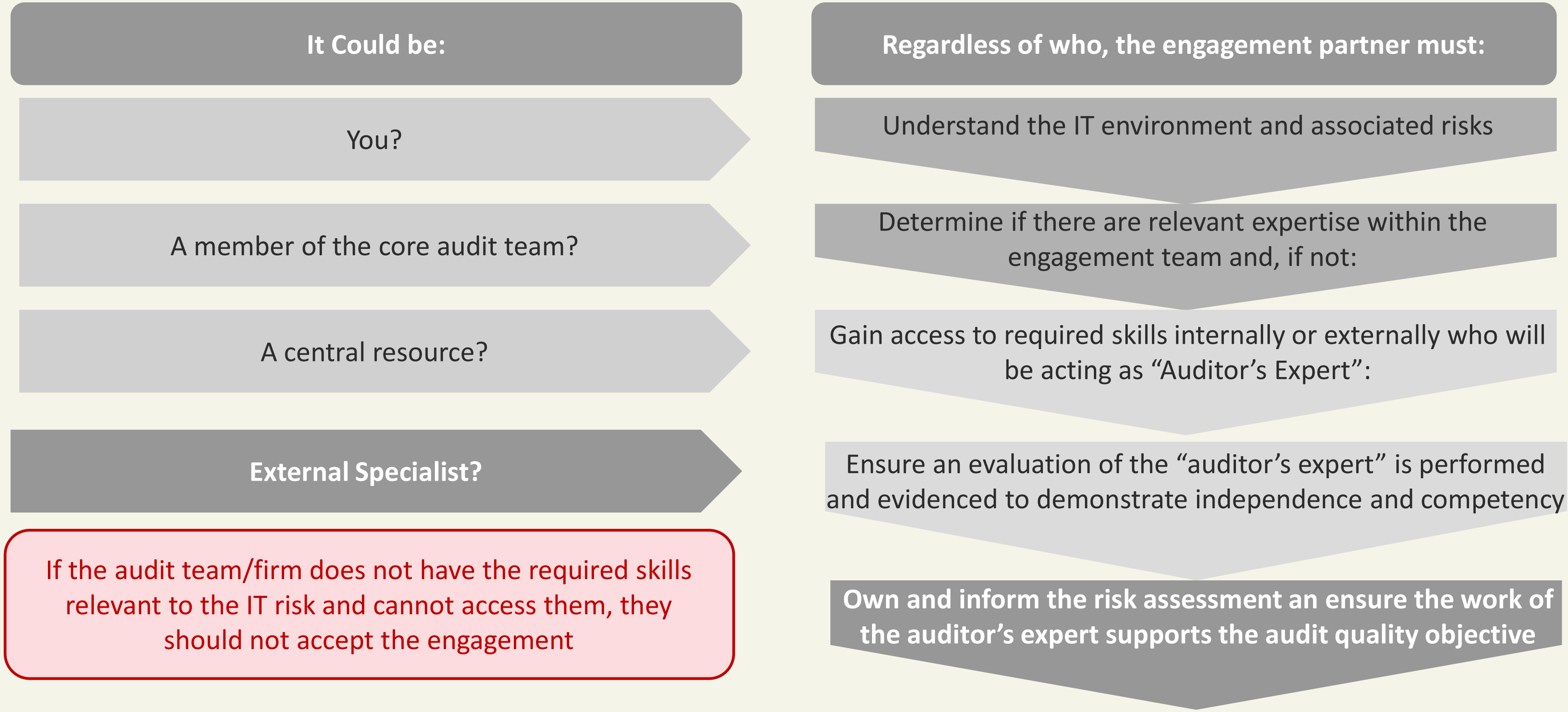
Checklists are an aide memoire – not evidence

Require a file note demonstrating critical thinking, scepticism and challenge support by evidence:

- Who?
- When?
- What?
- Screen shots?
- SLAs?
- SOC Reports?
- Accreditations
- Etc.

Ensure clear linkage to risk assessment and audit response

Who?



It Could be:

You?

A member of the core audit team?

A central resource?

External Specialist?

If the audit team/firm does not have the required skills relevant to the IT risk and cannot access them, they should not accept the engagement

Regardless of who, the engagement partner must:

Understand the IT environment and associated risks

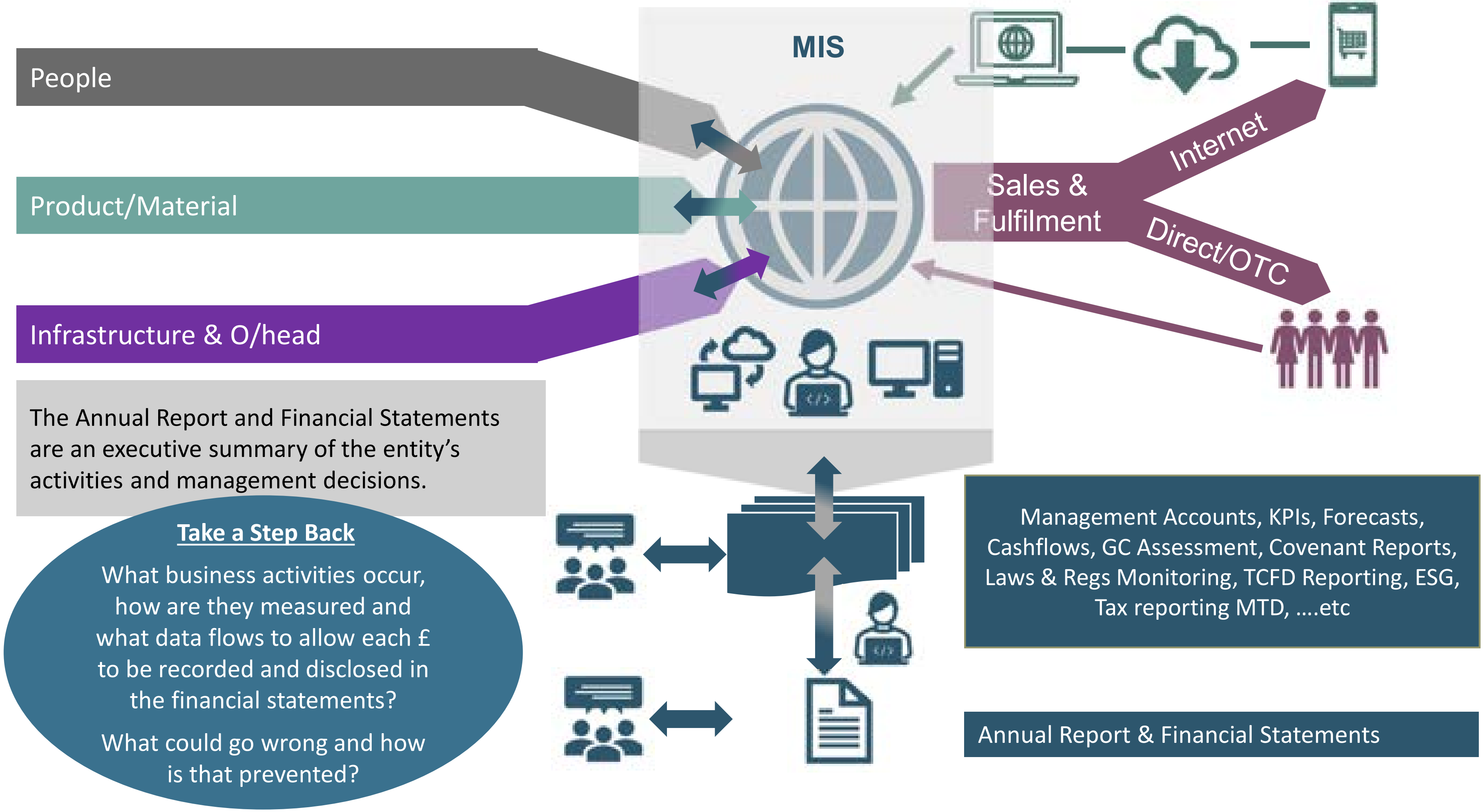
Determine if there are relevant expertise within the engagement team and, if not:

Gain access to required skills internally or externally who will be acting as "Auditor's Expert":

Ensure an evaluation of the "auditor's expert" is performed and evidenced to demonstrate independence and competency

Own and inform the risk assessment an ensure the work of the auditor's expert supports the audit quality objective

Business Model Illustration



The Annual Report and Financial Statements are an executive summary of the entity's activities and management decisions.

Take a Step Back

What business activities occur, how are they measured and what data flows to allow each £ to be recorded and disclosed in the financial statements?

What could go wrong and how is that prevented?

Management Accounts, KPIs, Forecasts, Cashflows, GC Assessment, Covenant Reports, Laws & Regs Monitoring, TCFD Reporting, ESG, Tax reporting MTD, ...etc

Annual Report & Financial Statements

People Costs

HR

- Hires & Fires
- Hours and Overtime
- Pay rates
- Productivity
- Performance & evaluation
- Laws and regulations

Payroll

Inhouse

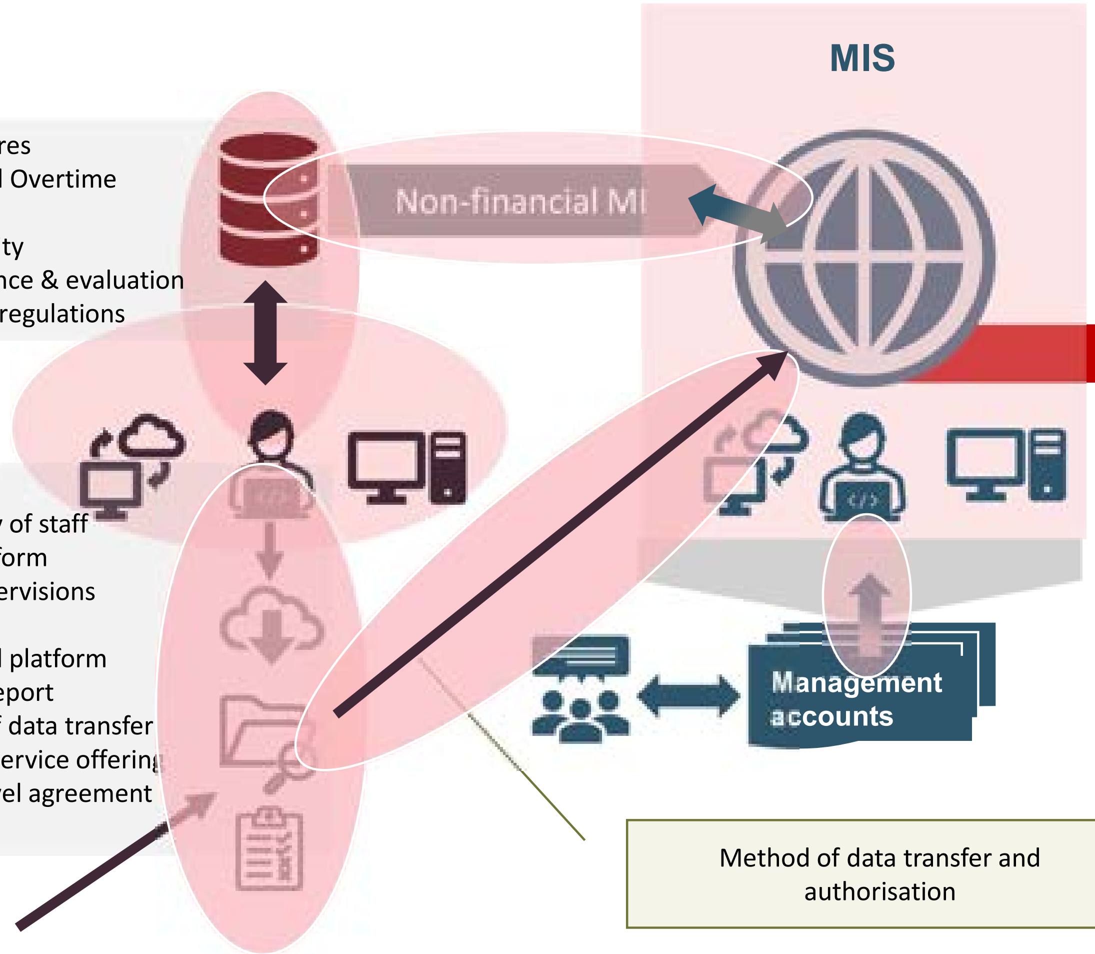
- Competency of staff
- Type of platform
- Level of supervisions

Outsourced

- Accredited platform
- Controls report
- Method of data transfer
- Extent of service offering
- Service level agreement
- Oversight

Finance

Cross check, approval, data transfer and payment run



Method of data transfer and authorisation

Cash out

🔴 = GITC and IT to Understand & Evaluate

Key GITC Considerations

- What format is the database?
- Who has access?
- Access security?
- Data transfer security?
- Change and access log?
- Change authorisation?

- Integrity of payroll platform?
- Who has access?
- Access security?
- How is it kept up to date?
- Change and access log?
- Change authorisation?
- Accreditations and Controls reports

ISA 402?

- Who has access?
- Access security?
- Authorisation security?
- How is data transferred?
- Manual vs automated cross checks
- Two factor verification

Revenue (Internet)

Sales Channel

- Customer ID and qualification
- Other fraud checks
- Order acceptance
- Automated /non-automated

Inventory

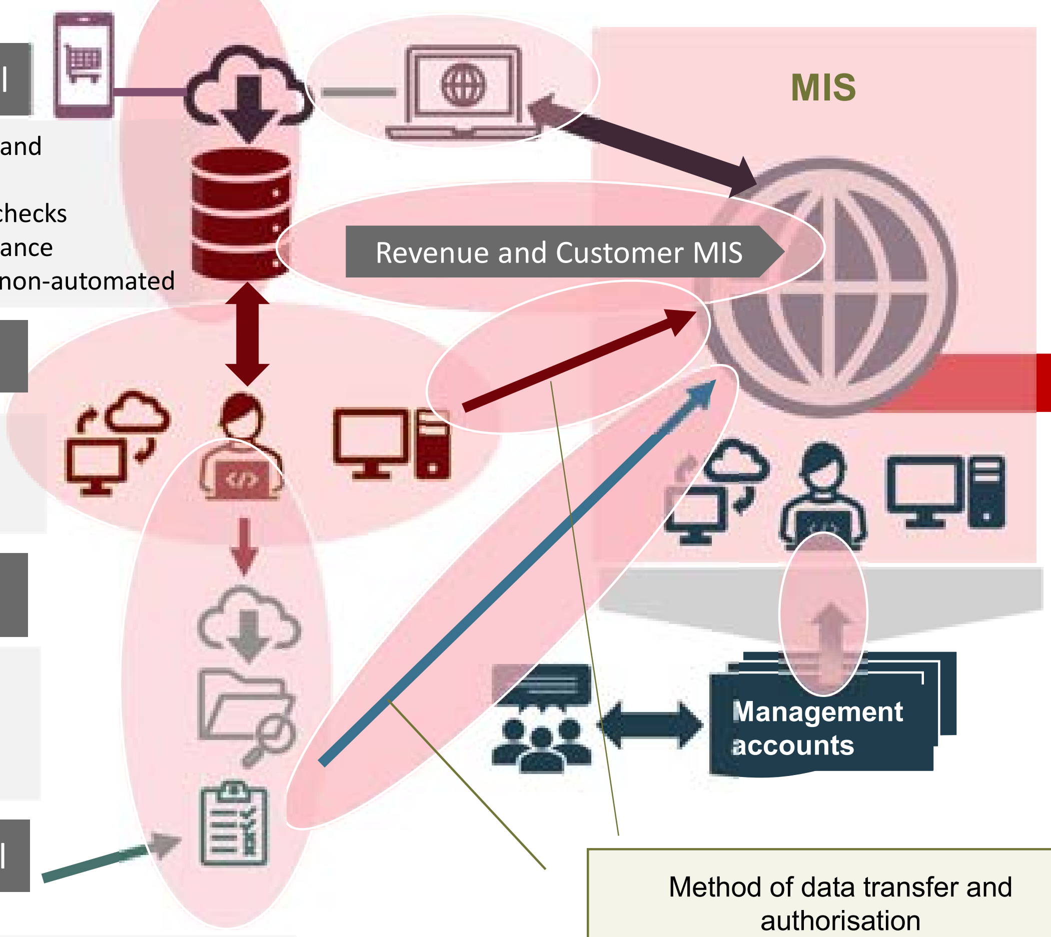
- Stock check and confirmation

Logistics & fulfilment

- Check and confirmation
- Dispatch and notification

Sales Channel

Cross check, confirmed sale, invoicing, data transfer, credit card notification, Credit control notification.



Method of data transfer and authorisation

● = IT and GITC to Understand & Evaluate

Key GITC Considerations

- Nature of internet hosting/in-house or third party ?
- Who has access?
- Access security?
- Data transfer security?
- Change and access log?
- Change authorisation?

Goods out and Cash in

Inventory, Logistics and fulfilment

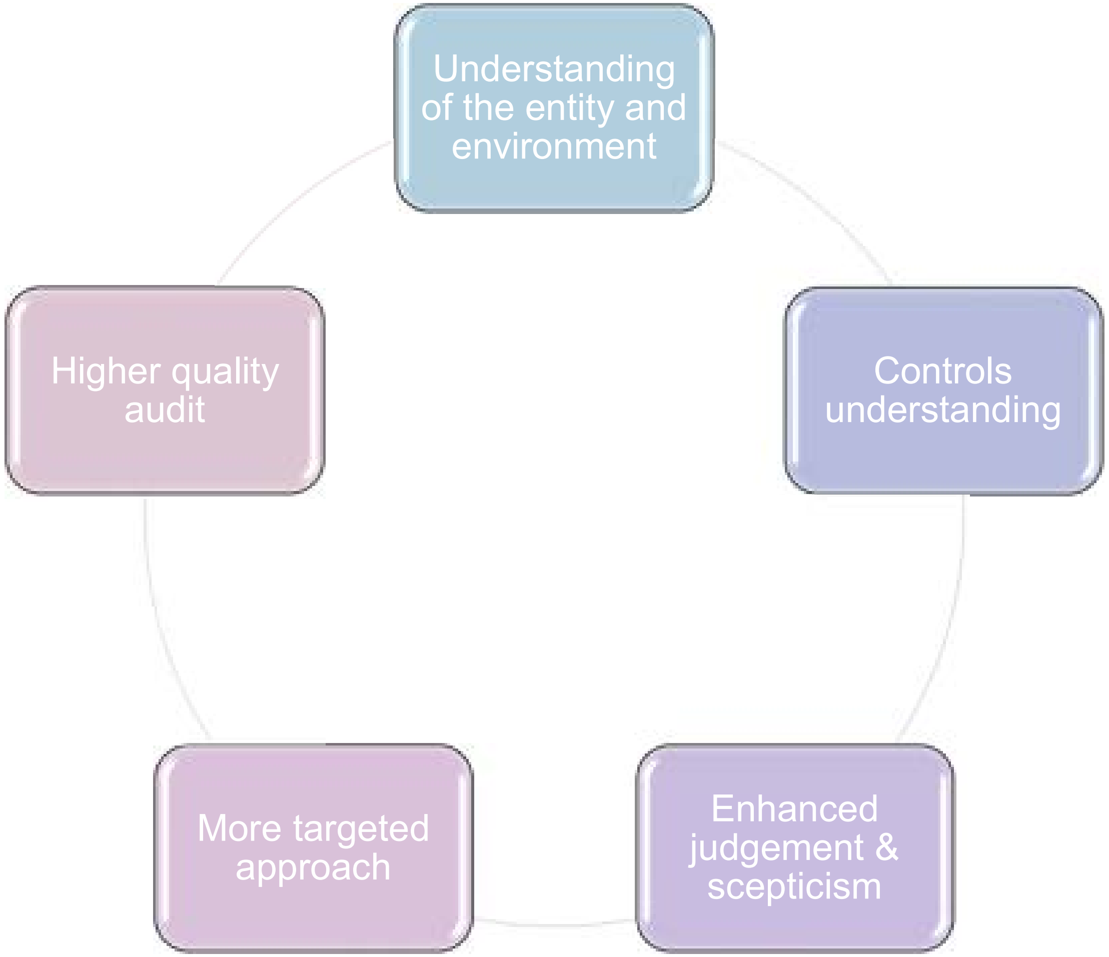
- Inhouse or outsourced
- Who has access?
- Access security?
- How is it kept up to date?
- Are checks automated or manual
- Change and access log?
- Exceptions reporting
- Reporting protocols
- Service level agreements

Potential area where:

- **substantive procedures alone aren’t enough**
- **Specialist input may be required**

Summing up

Benefits of ISA 315


Understanding of the entity and environment
Controls understanding
Enhanced judgement & scepticism
More targeted approach
Higher quality audit

Dos and Don'ts

DO

- Embrace the change – Win^3
- Remember who the real client is.
- Be professionally sceptical and mindful of your public interest obligation.
- Start with the business model and understand the environment in which the entity does business to support:
  - The identification of genuine risks;
  - The evaluation of controls, IT and GITCs
  - A more targeted approach, redeploying time to those areas that matter.
- Assess inherent risk on a gross basis.
- Be confident and use common sense (but know your comfort zone), drawing on your own experience.
- Be comfortable consulting and thinking outside of checklists
- Watch out for "end user applications" (aka Spreadsheets)
- Use flowcharts – a picture paints a 1,000 words
- Evidence your critical thinking and supporting information.
- Have the confidence to revise and refine your audit approach
- Enjoy the challenge and evidence your application of professional judgement and scepticism.
- Invest in your people

DO NOT

- Hide behind checklists in isolation
- Audit cliff dive or use a cookie cutter
- Allow SALY to work on your audits
- Evaluate IT in isolation
- Continue with a black box approach
- Take on engagements where you do not have access to the required IT expertise
- Miss out on the opportunity to evolve your audit approach

Tackle each year with a fresh perspective!

- Businesses evolve and their risk profile changes for internal and external factors
- Environment changes (e.g. Covid, Ukraine War)
- Our audit approach similarly needs to evolve - Evolution not revolution
- No more SALY!

What kind of auditor do you want to be?

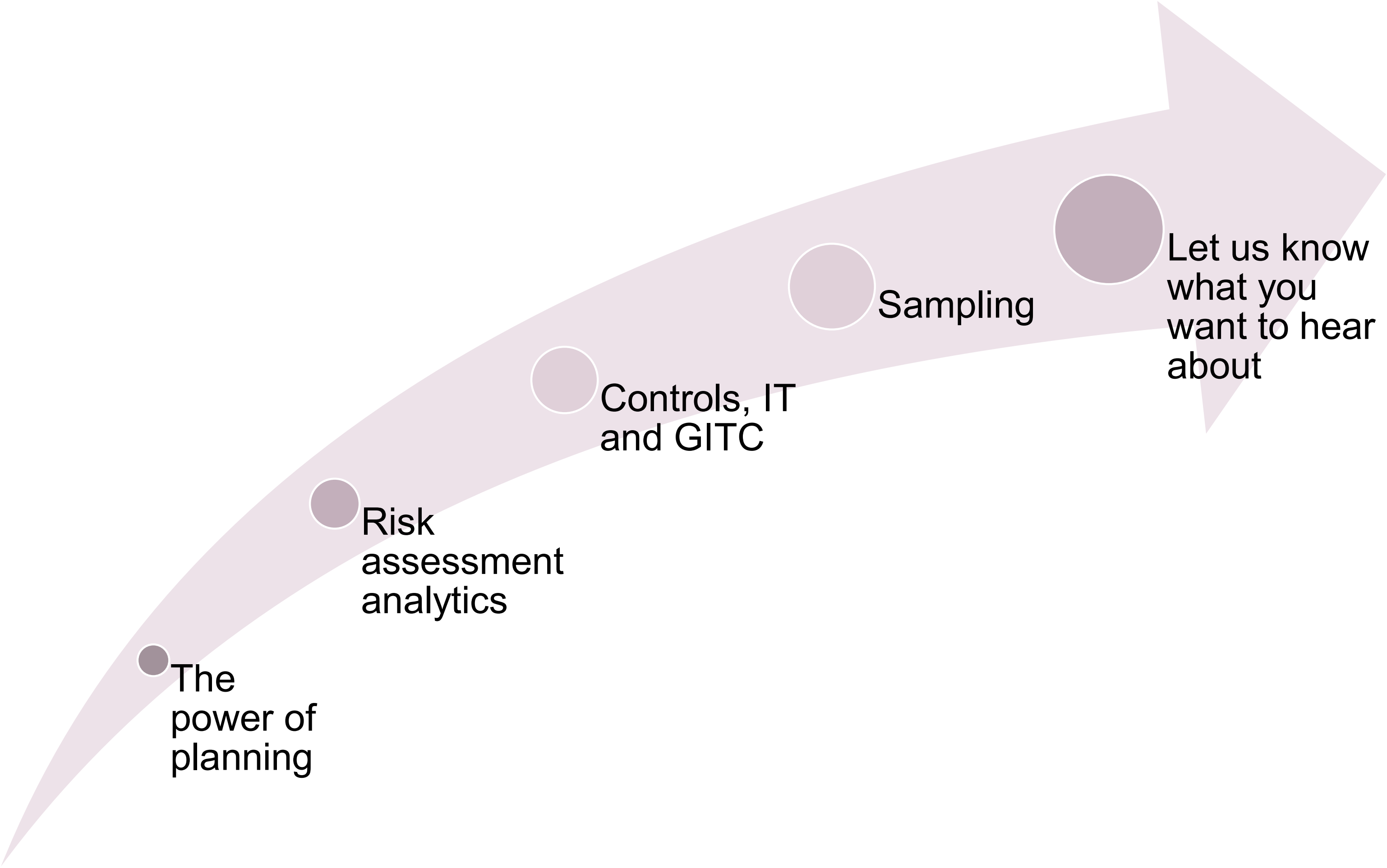
V

Real auditors don't need to know coding

Unless it's the Ethical Code!

What sort of auditors do the stakeholder of the entities we audit want?

To be continued....?



The power of planning

Risk assessment analytics

Controls, IT and GITC

Sampling

Let us know what you want to hear about

Thank you for attending

Please take the time to fill out our short survey:

Contact the Audit and Assurance Faculty

Phone: +44 (0)20 7920 8493

Email: tdaf@icaew.com

Web: icaew.com/AAF

This webinar is presented by the Audit and Assurance Faculty. Audit and Assurance Faculty membership provides you with the latest news and features direct to your inbox via our monthly Bulletin and Audit & Beyond eNewsletter.

For more information about faculty membership, please visit icaew.com/joinaaf.

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

ICAEW