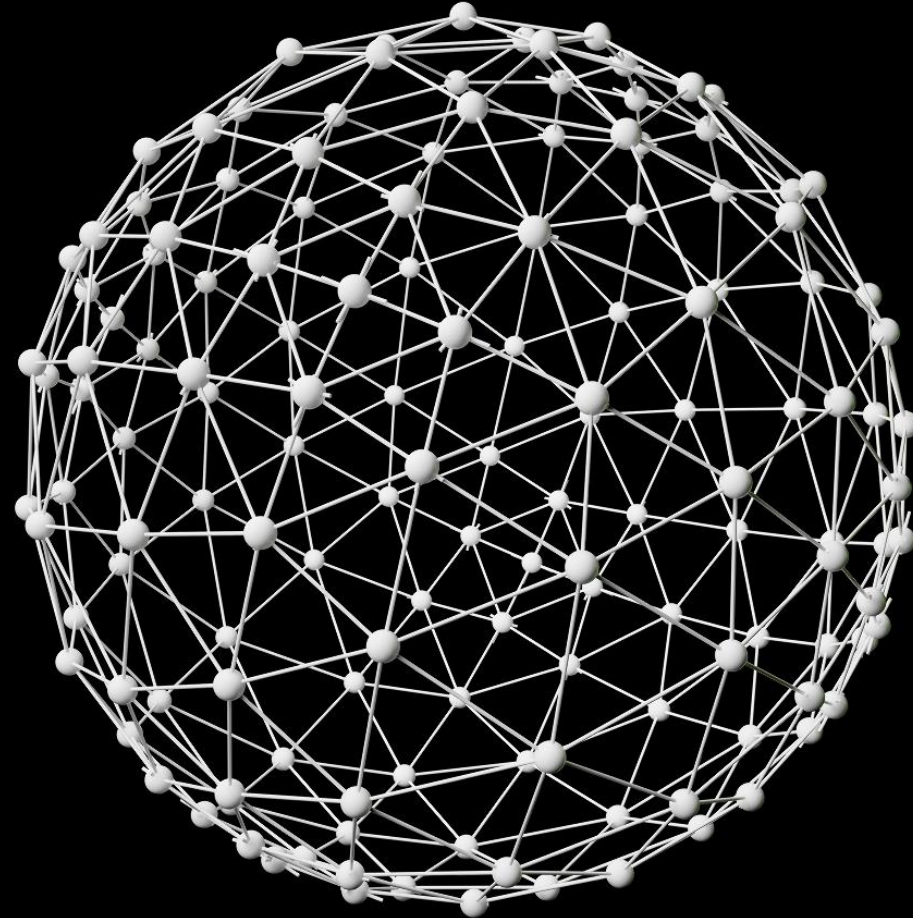


Deloitte.



Deloitte Finance Club Controls Forum

16 January 2020



Agenda

Welcome – Jon Thompson

The impact and likelihood of UK SOX – Sonya Butters and Michael Jones

The Future of Controls – Ani Sen Gupta

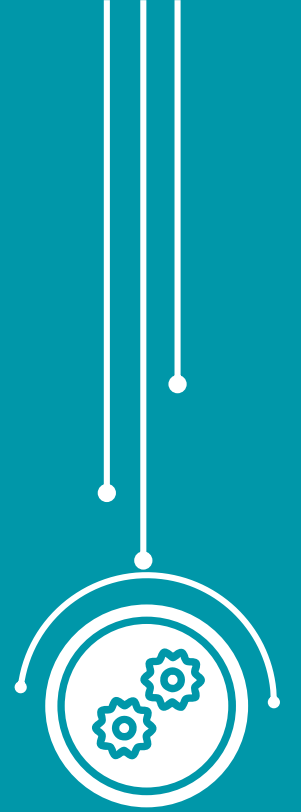
The Controls Hub – Ian Orgill

Q&A

Close and networking

The impact and likelihood of UK SOX

Sonya Butters & Michael Jones













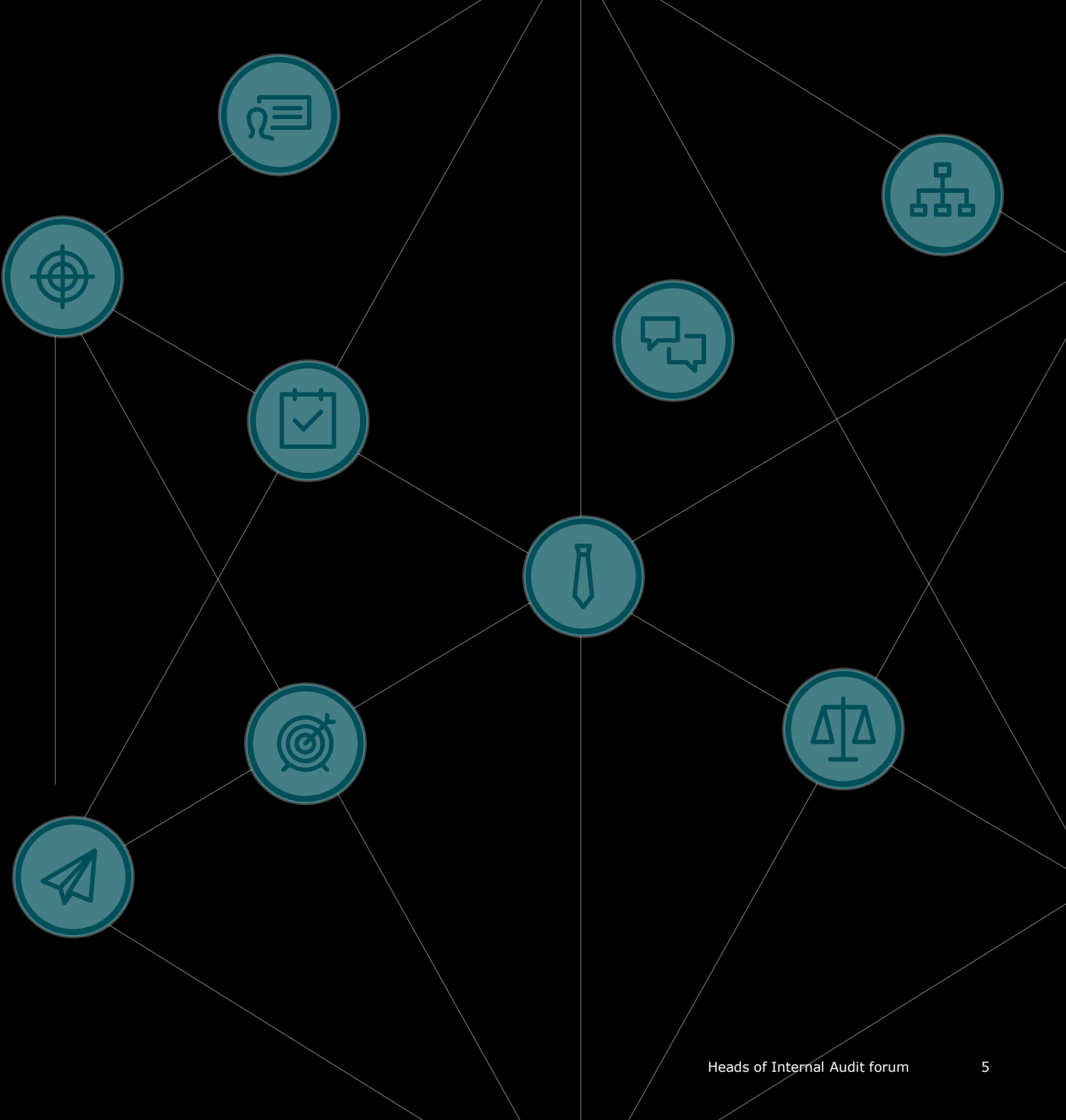
Internal Control Thoughts and insights

January 2020

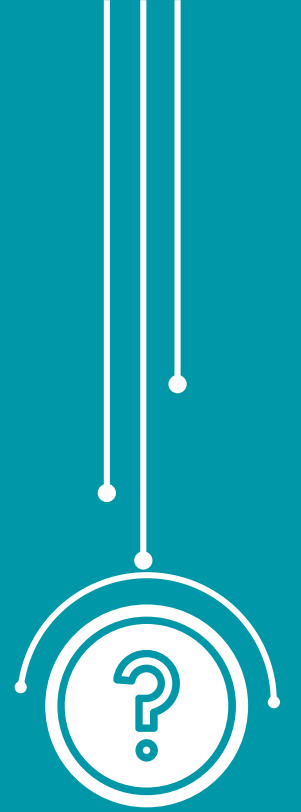
Internal financial controls

Agenda

-  UK internal control requirements
-  The current climate
-  The US experience
-  How does the UK compare
-  What do the auditors do
-  The BEIS consultation
-  Questions for management
-  Questions and discussion



Hands up



Put your hand up if you agree with the following statement

A

I have a good understanding of the UK Corporate Governance Code's requirements with regard to financial reporting ?

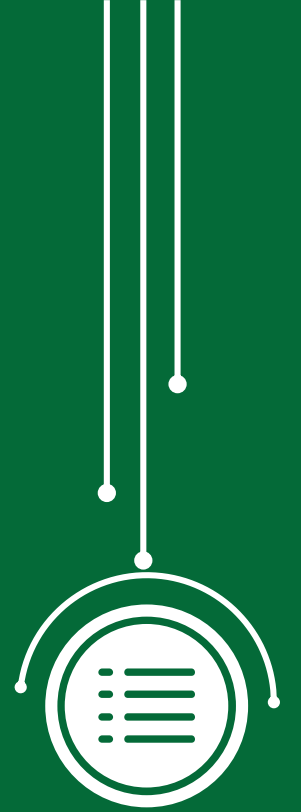
B

We fully comply with the UK Corporate Governance Code's requirements with regard to financial reporting

C

The UK Corporate Governance Code is an effective framework to prevent financial reporting errors

UK internal control requirements



UK current requirements

Principles are in place, implementation varies

| Applies to: | All companies | Companies listing in the UK | Premium listed companies |
|---------------------|---|---|--|
| Rules | Companies Act 2006 | Listing Rules require a Sponsor's Declaration, after "due and careful enquiry" to the Regulator on IPO | <ul style="list-style-type: none"> Comply with the Principles of the UK Code Provisions of the Code: comply or explain |
| Requirements | <ul style="list-style-type: none"> "Keeping adequate accounting records" "safe guarding the assets of the company" "taking reasonable steps for the prevention and detection of fraud" | "the directors of the applicant have established procedures which provide a reasonable basis for them to make proper judgments on an ongoing basis as to the financial position and prospects of the applicant and its group" | Principle: "The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives." |
| Guidance | None | ICAEW Tech 14/14 | FRC's 2014 Guidance on Risk Management and Internal Control |
| Focus | None | <ul style="list-style-type: none"> Forward looking Reporting to the Board and to the market | <ul style="list-style-type: none"> Operational, financial and compliance controls Principal risks |

Monitoring risk management and internal control

Provisions of the Code – comply or explain

The board should monitor the company's risk management and internal control and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

UK Corporate Governance Code Provisions

The board should consider on an ongoing basis (FRC 2014 Guidance) :

How effectively have risks been assessed and the principal risks determined?

How have the principal risks been managed or mitigated?

Have necessary actions been taken promptly to remedy any significant failings or weaknesses?

Do the causes of the failing or weakness indicate poor decision making?

Are emerging issues being monitored effectively and can procedures be readily reported?

Questions for Boards to consider:

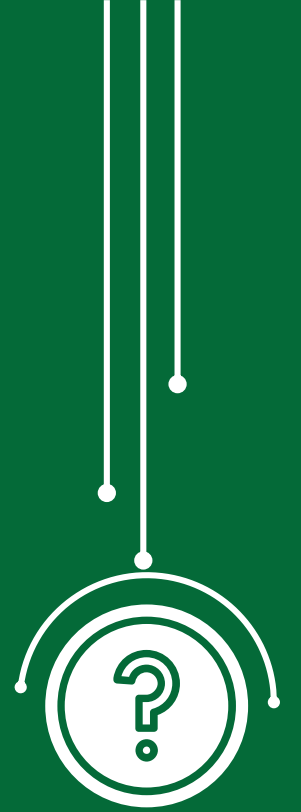
Have you defined "material financial controls" for your business?

Does the board have visibility of the "material financial controls"?

Have you defined a significant failing or weakness ?

Have you considered culture and whether it is embedded?

Is it working?



Why is this important?



£1.50 (Ch. Month £2.00)
Tuesday 23.06.14
Published in London
and Manchester
guardian.com

the guardian

£2bn shares slide as Tesco admits overstating profits

Miliband: tax on tobacco giants will boost NHS

Newspaper of the year
Winner of the
Pulitzer prize

FINANCIAL TIMES

Kier blames debt increase on accounting error

Shares tumble after outsourcing specialist adds £50m of borrowing for half year to December

FINANCIAL TIMES

Patisserie Valerie halts trading in its shares

Board suspends chief financial officer and discloses 'potentially fraudulent' practices

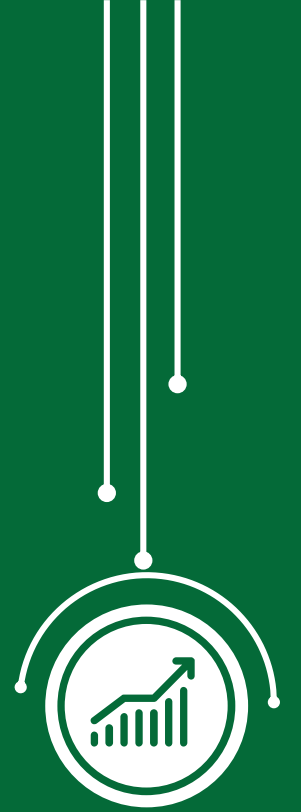
"I know I was not dishonest. I was unaware of fraud," he wrote, saying he had no knowledge of the serious accounting irregularities that have since come to light, describing himself as a hands-off owner.

Yet Mr Johnson was the company's executive chairman at the time so bore some responsibility for overseeing its management and performance.



British chiefs in firing line over BT accounting fraud scandal in Italy

**A growing call that more
needs to be done...**



Reforming the FRC and the UK audit market

Audit committees have come in for some criticism

Extracts from the CMA's Final Report

"...the evidence...suggests there is significant variation in the performance of Audit Committees within the FTSE 350...there is a persistent problem of variable and sometimes poor audit quality. Therefore, this remedy is primarily aimed at improving underperforming Audit Committees...."

Para 5.2

"...equally worrying is the finding that many audit committees are spending so little time on auditing matters. This questions whether many audit committees are committed to challenging management and to putting in the necessary time to ensure that auditors are as well."

What BEIS has to say

The Future of Audit, BEIS, April 2019



“The Review recommended that **serious consideration should be given to introducing a Sarbanes-Oxley (SOX) regime in the UK**. This would require the CEOs and CFOs of public companies to report on the effectiveness of a company’s financial reporting and internal controls, with the **board and management having clear responsibility for the** accuracy of reporting and **robustness of controls.**”

Reforming the FRC and the UK audit market

Next steps – our best guess

December
2019



Sir Donald Brydon @BrydonDonald · Dec 18

Delighted by positive reaction to [#BrydonReview](#) today. [#auditors](#) to be obliged to act in the public interest and have regard to the interests of users of their report beyond solely those of shareholders. gov.uk/government/pub...

Q1 2020

We expect to BEIS to issue a follow-up consultation on matters such as:

- UK SarbOx
- Definition of public interest entities
- Enforcement regime for holding relevant directors to account
- CMA proposals

By end
2020

We expect a consultation on revisions to the Companies Act to deliver the reforms

The Brydon Report – recommendations focused on companies

The topics covered

- **Accounting records**
- **Internal controls**
- **Risk reporting**
- True & fair
- Judgements
- Reporting performance
- Payment practices
- Resilience
- Capital maintenance
- **Whistleblowing**
- **Fraud prevention & detection**

New reporting by directors in the annual report

- Resilience Statement
- Public Interest Statement
- **Statement that CEO/CFO internal control attestation received**
- **Actions taken to prevent and detect material fraud**
- Response to external signals of concern
- Appropriateness of dividend payment
- Payment policies and performance
- **Risk reporting published prior to audit plan**

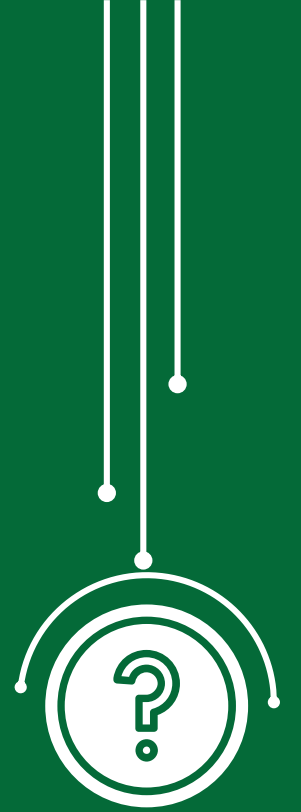
Internal controls

- **Attestation by CEO and CFO to the board on effectiveness of internal financial reporting controls**

Audit and Assurance Policy

- Published by the audit committee and subject to annual advisory vote by shareholders
- Developed with input from shareholders and the workforce

What does Brydon say about internal control...



The chapters on accounting records and fraud are important context

Chapter 12 - Accounting Records

12.1 ...s386 CA06 requires all companies to keep adequate accounting records

12.3 auditors already have an obligation to state "whether a company in their opinion has kept adequate accounting records"

12.4 I recommend the Government review the Companies Act to...clarify...what is meant by "adequate accounting records"

12.8 I recommend ARGA develop guidance for auditors around their responsibilities in relation to accounting records.

Chapter 14 - Fraud

Current requirements are confusing...so make the auditors role re fraud clear...

14.1.5 ...make clear it is the obligation of an auditor to endeavour to detect material fraud in all reasonable ways.

Recommends new directors' statement:

14.2.2...the directors should report on the actions they have taken to fulfil their obligations to prevent and detect material fraud against the background of their fraud risk assessment

Plus auditors should report "explicitly the work performed to conclude whether the directors' statement...is appropriate..[and]...state what steps they have taken to assess the effectiveness of the relevant controls..."

Chapter 13 - Introducing "UK SOX" with the emphasis on directors' responsibilities

Background...SOX is positive...but remember current UK Corporate Governance Code requirements...which we are poor at enforcing...

13.1.4 It is widely agreed...*"the extent and nature of work performed in support of these requirements and reporting obligations varies and usually does not involve detailed testing of the effectiveness of controls."*

...but there's wide support for SOX.

Plans to introduce CEO & CFO attestation...

13.1.8 ...Government gives...consideration to a UK Internal Controls Statement consisting of a signed attestation by the CEO and CFO to the Board that an evaluation of the effectiveness of the company's internal controls over financial reporting has been completed...

13.1.9 ...a company would not normally be required to have the attestation audited. However, a failure of relevant controls in the 12 months prior / 12 months following the attestation should result in a requirement for future statements to be audited for...three years...

...and develop guidance...

13.1.11 ...the ACCIF develops principles that should be followed by CEOs and CFOs in making an internal controls effectiveness attestation.

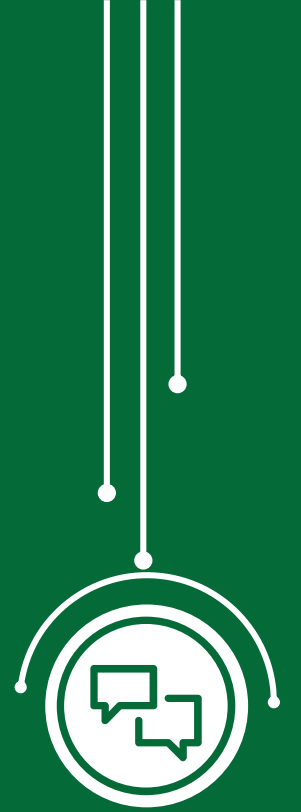
...including what to do if there are weaknesses...

13.1.12 Where weaknesses...in controls have been reported it should become an obligation on directors to report on what remedial action has been taken... Where [a] material weakness persists over two reporting periods, boards should...have their attestations audited...

...but we don't need more on ELCs...

13.1.13 ...boards...are required to monitor the company's risk management and internal control systems...boards should make clear what processes have been considered and reasons for their confidence in their effectiveness. ...it would be a step too far to extend the proposed UK Internal Controls Statement to entity-level controls.

Let's talk about Sarbanes Oxley



Introduction to SOX

The Sarbanes-Oxley Act (SOX) became law in the US in July 2002 and addresses Internal Controls over Financial Reporting "ICFR"

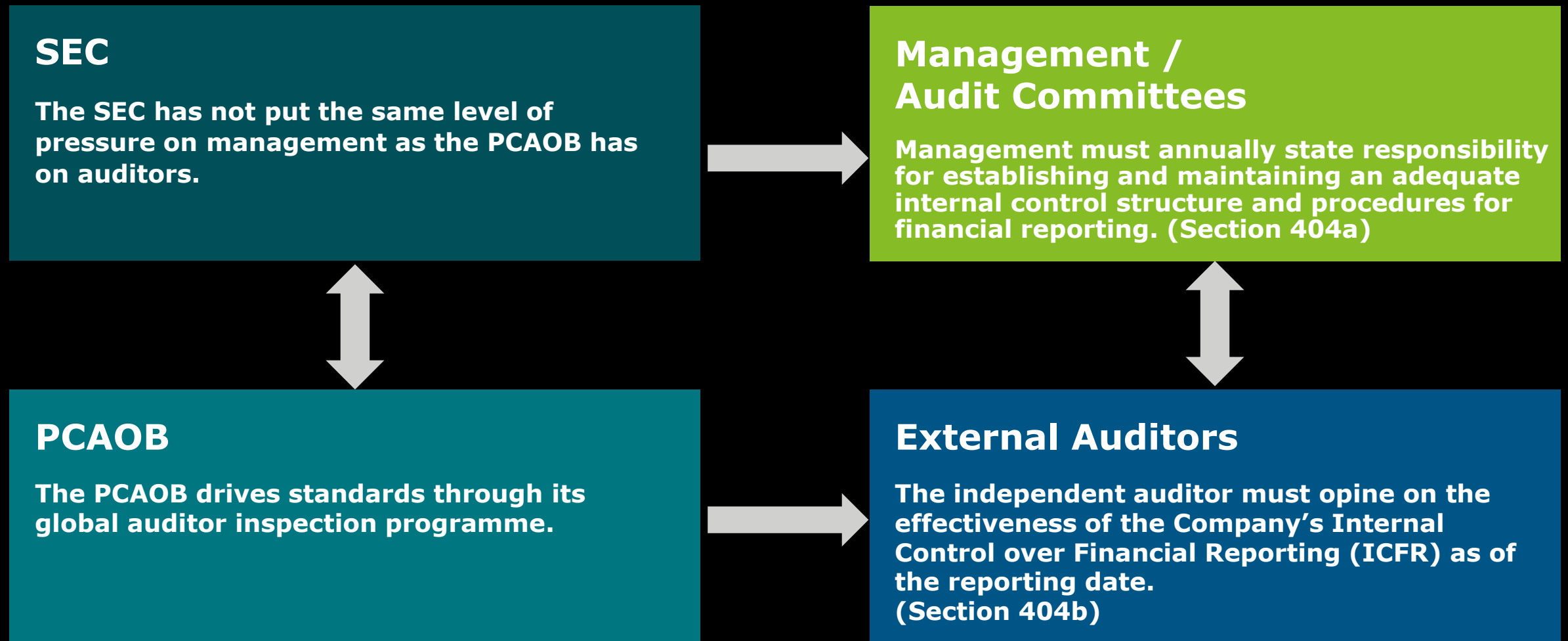


Enron was named "America's Most Innovative Company" by the magazine Fortune for six consecutive years.

WorldCom was the United States' second largest long distance phone company.



Increased focus from all sides



Types of controls needed to comply with SOX

Entity-level controls (ELCs)

Code of conduct, HR recruitment policies, period-end financial reporting process.

Process-level controls (PLCs)

Manual examples include: bank reconciliations, inventory counts, review of aged debtors.
Automated examples include: three way match of purchase order, to invoice, to GRN.

General IT controls (GITCs)

Access controls that restrict the ability of unauthorised users to amend certain records or documents.

COSO's Internal Control – Integrated Framework (2013)

1. 5 components of internal control that need to be present and operating together.
2. Further broken down into 17 principles across those components that need to be met.
3. Provides specific points of focus as a guide to help address the 17 principles.

Control environment

1. Demonstrates commitment to integrity and ethical values.
2. Exercises oversight responsibilities.
3. Establishes structure, authority, and responsibility.
4. Demonstrates commitment to competence.
5. Enforces accountability.

Risk assessment

6. Specifies suitable objectives.
7. Identifies and analyzes risk.
8. Assesses fraud risk
9. Identifies and analyzes significant change.

Control activities

10. Selects and develops control activities.
11. Selects and develops general controls over technology.
12. Deploys through policies and procedures.

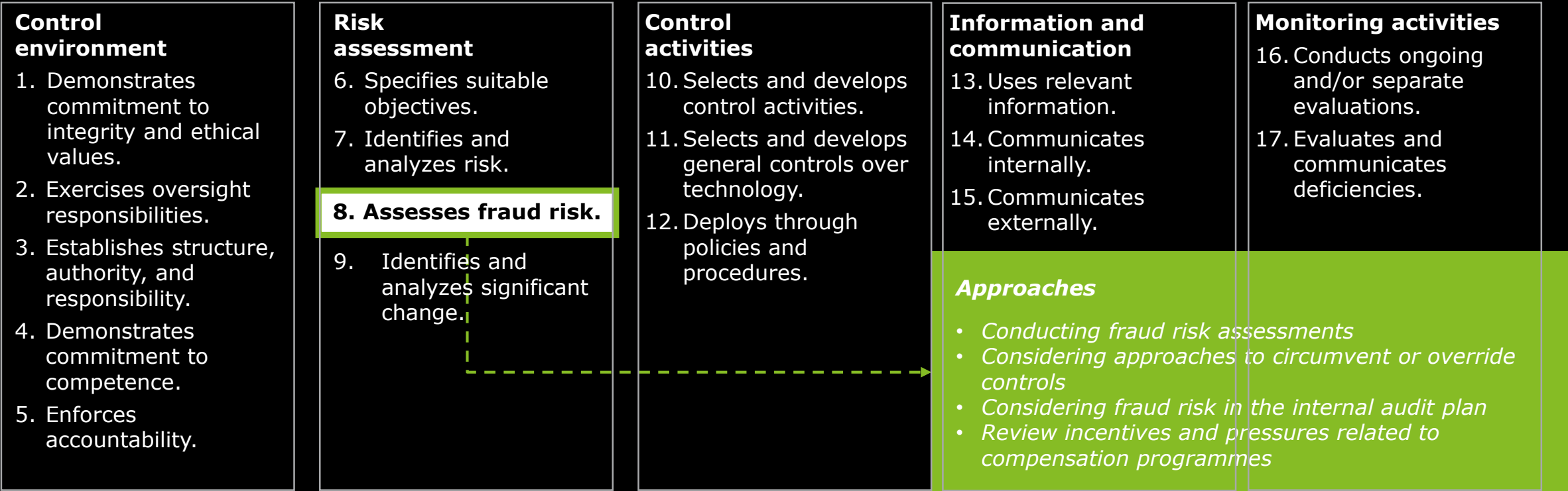
Information & Communication

13. Uses relevant information.
14. Communicates internally.
15. Communicates externally.

Monitoring activities

16. Conducts ongoing and/or separate evaluations.
17. Evaluates and communicates deficiencies.

COSO's Internal Control – Integrated Framework (2013)



Questions for Boards to consider:

Is there benefit in a generally recognised framework to help define what good looks like?

Should you have a Board conversation about the application of COSO or a similar framework?

What's all the fuss about?

Intellectually robust, but the devil is in the detail...

**Scoping is complex
and judgemental**

**Significant
documentation
/resource
requirements**

**Includes central
functions (tax /
treasury etc)**

GITC is challenging

Some of the concepts are challenging...

**Report dependant
controls**

**Management
review controls**

**Outsource
providers**

IT Controls – Why are they so important?

Your IT environment and in turn the controls over this are the fundamental building block upon which your internal control environment is built.

Business are ever more reliant upon their IT systems to operate the business, interact with customers and suppliers and produce financial statements.

Effective control over IT is critical in ensuring...

Security

Ensuring that your systems and data are secure and appropriately protected from the risk of unauthorised access.

Integrity

Ensuring that your systems are functioning as intended and you can rely of the accuracy and completeness of processing.

Availability

Ensuring the resilience and redundancy of your environment to support ongoing operation and organisational viability.

Questions for Boards to consider:

How do you get assurance over the effectiveness of your IT controls?

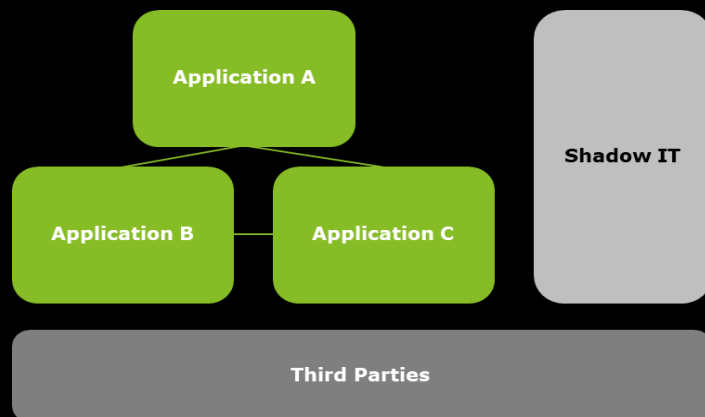
How integrated are your IT controls into your overarching internal control framework?

IT Controls – Why are they challenging to get right?

There are multiple challenges associated with implementing an effective IT control environment.

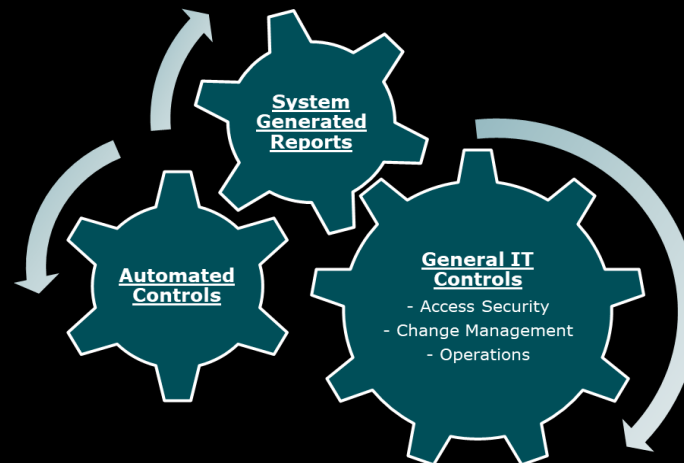
Complexity of IT Environment

Understanding your IT environment, the systems you use and the criticality of these can be challenging. This is complicated by the use of “shadow IT” and employing third parties to support and operate your environment.



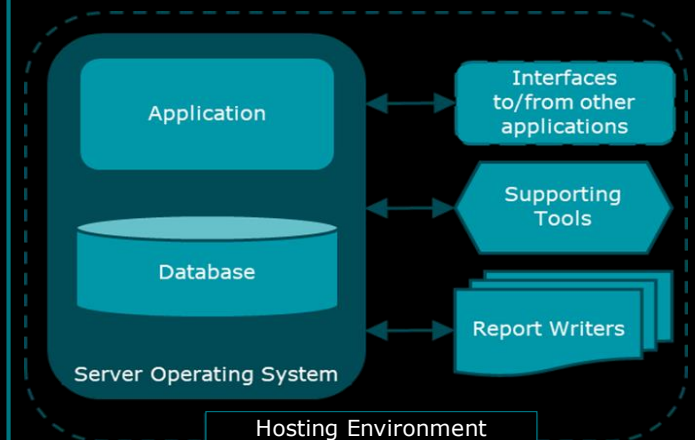
Interdependency of Controls

There are multiple layers of IT controls which need to be deployed across the environment and need to operate in tandem to ensure appropriate levels of control on multiple different systems.



Multiple Layers of IT

Controls need to be implemented and operated across the multiple layers of the environment, in particular the infrastructure supporting each of your key applications.



IT Controls – What can go wrong?

A real world example...

- Large manufacturing business who, due to legacy technology, purchased raw materials in kg, but created self-bill-invoices in tons, requiring a price factoring of 1000 at point of invoice creation.
- Minor “efficiency” change made to systems to fix unit of measure – inappropriately controlled, resulting in a payment of £70k being incorrectly factored to £70m and paid.
- Controls which could have prevented the issue:

Change Management

If the change had passed through an effective change management process, the change would have been tested and the potential downstream impact identified and appropriately remediated.

Restriction of Access

If the ability to make the change was limited to appropriate individuals, the residual impact would have been identified and adherence to the change management process enforced.

Payment Limits

If an automated control was in place to ensure payments above a certain value were blocked until specific senior approval was provided, the payment would not have left the business.

Questions for Boards to consider:

Are you clear on your inventory of systems?

How do you control “shadow IT” and monitor controls operated by third parties?

Do you have a control in place to limit the size of payment which can leave the business?

Is all the hard work worth it?

**Reissuance restatements are down c. 30%
(2009 – 2017).**

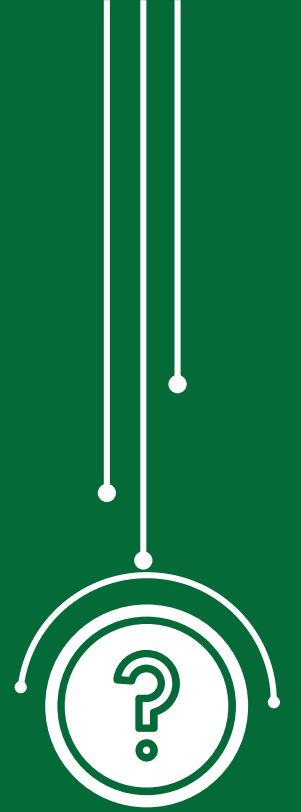
(source: auditanalytics.com)

**“The cost of equity and the cost of debt
capital are significantly lower for those
companies choosing to have their internal
controls audited.”**

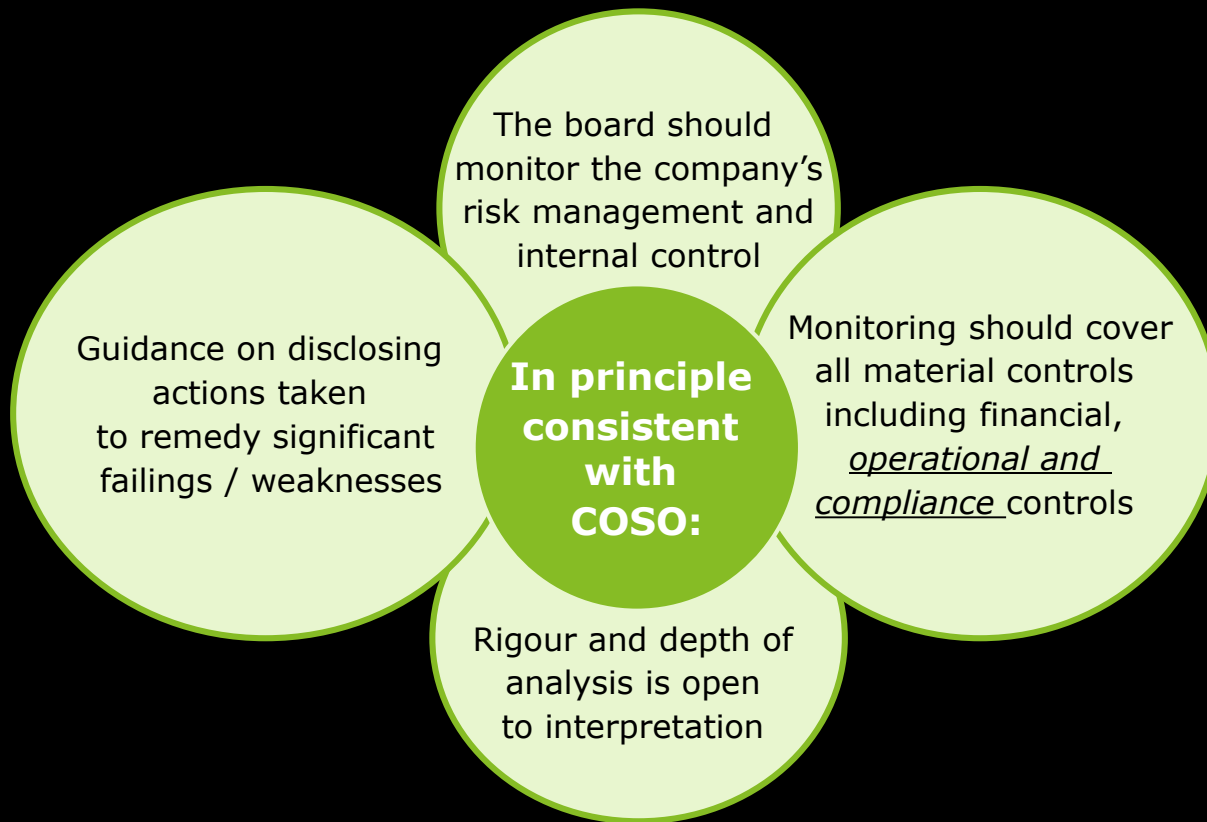
*(Cassell, Cory A. and Myers, Linda A. and Zhou, Jian, The Effect of Voluntary
Internal Control Audits on the Cost of Capital)*



The UK approach: how does it compare...



UK approach in comparison



The UK Corporate Governance Code (The Code) and related FRC Guidance require a risk based approach and 'comply or explain'.

In the UK, listed boards make an annual statement on how they have applied the principles of the Code.

SOX requires senior executives, typically CEO and CFO, to certify the effectiveness of controls over financial reporting.

As part of an IPO directors must assert "*they have established procedures which provide a reasonable basis for making proper judgements...as to the financial position and prospects of the company*".

In theory both principles based; in practice there is simply more history and regulation in the US

Questions for Boards to consider:

If something went wrong how comfortable would you be in explaining your monitoring process after the event?

How do UK companies shape up

Poorly, although few would admit to it...



Few undertake a detailed financial risk assessment.



Little evaluation of entity level controls.



Limited identification of material / key controls.



Limited analysis of risk and control within central functions.



Documentation is poor.



Lack of accountability – process / control owners.

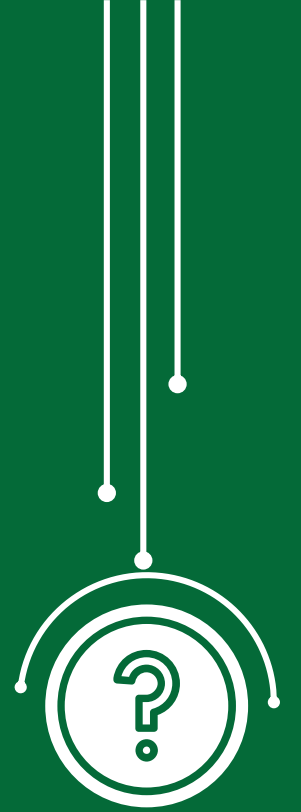


Lack of focus on GITC.



Little evidence that controls are operating as designed.

What do the auditors do?



What do the auditors do ?

Possibly less than you think...

Auditing Standards require design and implementation of controls over significant risks to be tested. All incremental testing is a matter of the auditors judgement.

The auditor must tell you about the significant deficiencies they found in the course of their work, but the scope of that work may be limited....

"The auditor shall **obtain an understanding** of internal control **relevant to the audit...not all controls that relate to financial reporting** are relevant to the audit. It is a matter of the auditor's professional judgment"

"...the auditor shall obtain an understanding of...whether the entity has **designed and implemented controls** for **significant risks...**"

(ISA 315)

"The auditor shall design and perform tests of...the operating effectiveness of **relevant** controls **if**:

- The auditor's assessment....**includes an expectation that the controls are operating effectively**; or
- Substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level."

(ISA 330)

"...The auditor shall **communicate in writing** significant deficiencies in internal control identified during the audit to those charged with governance on a timely basis"

(ISA 265)

Questions for your auditors



Which of our controls do you consider to be relevant, by process and by function?



Do we have controls which you elect not to test because you believe they are not operating effectively?

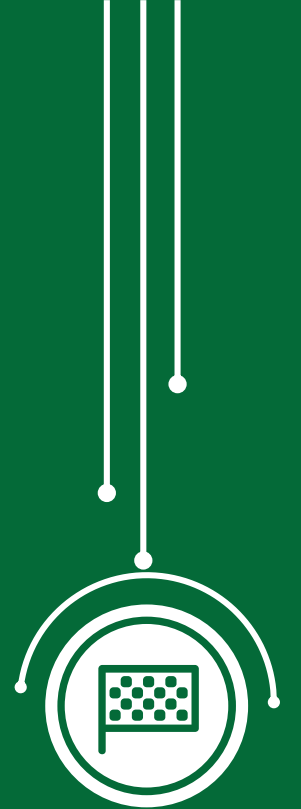


How does the narrative in our Annual Report on controls compare to best practice?



What do you plan to publically report this year end as your observations on internal control?

Get ready for the BEIS Consultation



Matters to consider in responding to the BEIS consultation this Autumn

**Board
delegation
of authority**

**Identification
and testing
of entity level
controls**

**Financial risk
assessment**

**Fraud risk
assessment**

**Identification
of material
financial
controls**

Where should UK plc be on the controls continuum?

**Robust
process
documentation
and clear process
ownership**

**Identification of
general
IT ccontrols**

**Testing
of design /
operating
effectiveness by
management**

**Agreed
definition
of a significant
failure or
weakness**

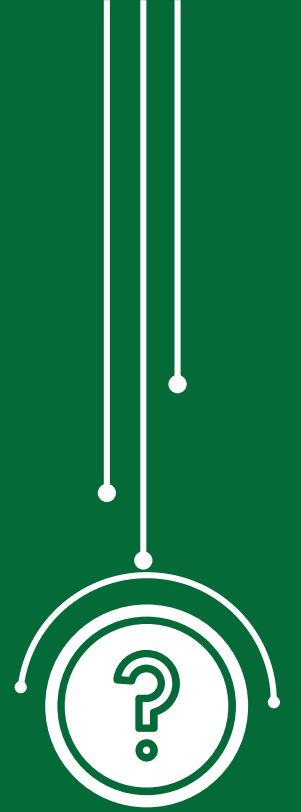
**Sign off
by management**

Questions for Boards to consider:

Consider where you are and where you want to be, with regard to these criteria ?

What would be an appropriate regulatory framework ?

Questions to pose now...



Questions for management



Is there a clear link between the principal risks related to financial reporting and second / third line assurance activity in your organisation?



Can management provide an annual analysis of material controls by process / central function and how they are assured?

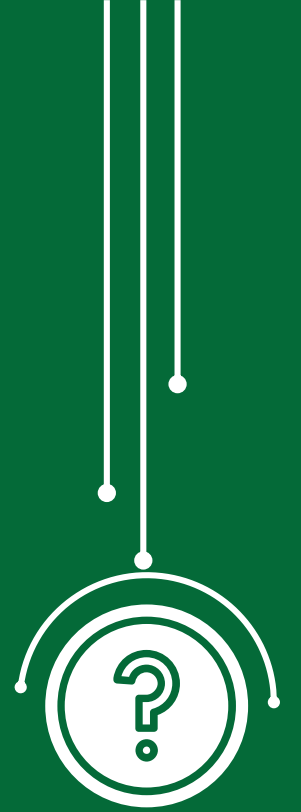


Has management undertaken a fraud risk analysis, including the risk of fraud in financial reporting?



Is there clarity over which IT systems are in-scope for financial reporting purposes? Ask for evidence general IT controls have been tested.

and finally...a question for you



Put your hand-up if you agree with the following statement

A

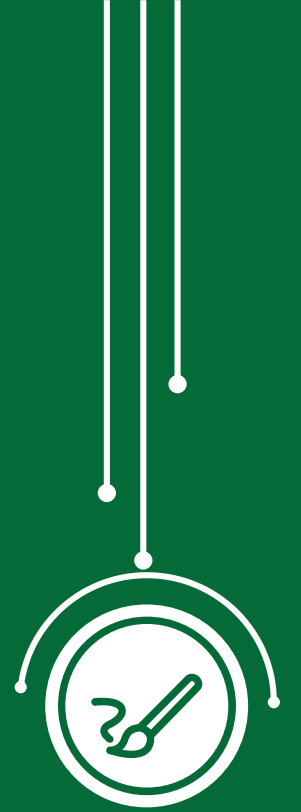
The application of a detailed framework, such as COSO, would improve financial reporting standards in the UK.

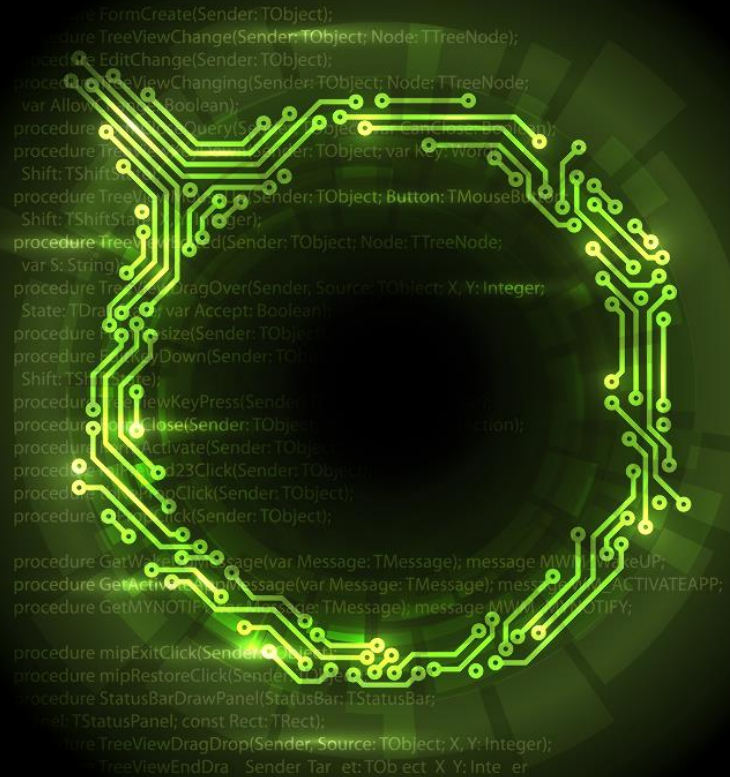
B

I would support the introduction of UK SOX.

The Future of Controls

Ani Sen Gupta and Ian Orgill





```
procedure FormCreate(Sender: TObject);
procedure TreeViewChange(Sender: TObject; Node: TTreeNode);
procedure TreeViewEditChange(Sender: TObject);
procedure TreeViewViewChanging(Sender: TObject; Node: TTreeNode;
  AllowCancel: Boolean);
procedure TreeViewQuery(Sender: TObject; var Cancel: Boolean);
procedure TreeViewMouseDown(Sender: TObject; var Key: Word;
  Shift: TShiftState);
procedure TreeViewMouseUp(Sender: TObject; Button: TMouseButton;
  Shift: TShiftState);
procedure TreeViewMouseDown(Sender: TObject; Node: TTreeNode;
  var S: String);
procedure TreeViewDragOver(Sender, Source: TObject; X, Y: Integer;
  State: TDragState; var Accept: Boolean);
procedure TreeViewResize(Sender: TObject);
procedure TreeViewKeyDown(Sender: TObject; var Key: Word;
  Shift: TShiftState);
procedure TreeViewNewKeyPress(Sender: TObject; var Key: Char);
procedure TreeViewClose(Sender: TObject; var Operation: Boolean);
procedure TreeViewActivate(Sender: TObject);
procedure TreeViewD23Click(Sender: TObject);
procedure TreeViewUpClick(Sender: TObject);
procedure TreeViewDownClick(Sender: TObject);

procedure GetWindowsMessage(var Message: TMessage); message MWL_COMMAND;
procedure GetActiveWindowMessage(var Message: TMessage); message MWL_ACTIVATEAPP;
procedure GetMyNotifyMessage(var Message: TMessage); message MWL_NOTIFY;

procedure mipExitClick(Sender: TObject);
procedure mipRestoreClick(Sender: TObject);
procedure StatusBarDrawPanel(StatusBar: TStatusBar;
  Panel: TStatusPanel; const Rect: TRect);
procedure TreeViewDragDrop(Sender, Source: TObject; X, Y: Integer);
procedure TreeViewEndDrag(Sender, Target: TObject; X, Y: Integer);
```

“Are **today's controls** up to
the job?”

Misalignment with business and risk objectives ... too many controls

Redundant and overlapping controls

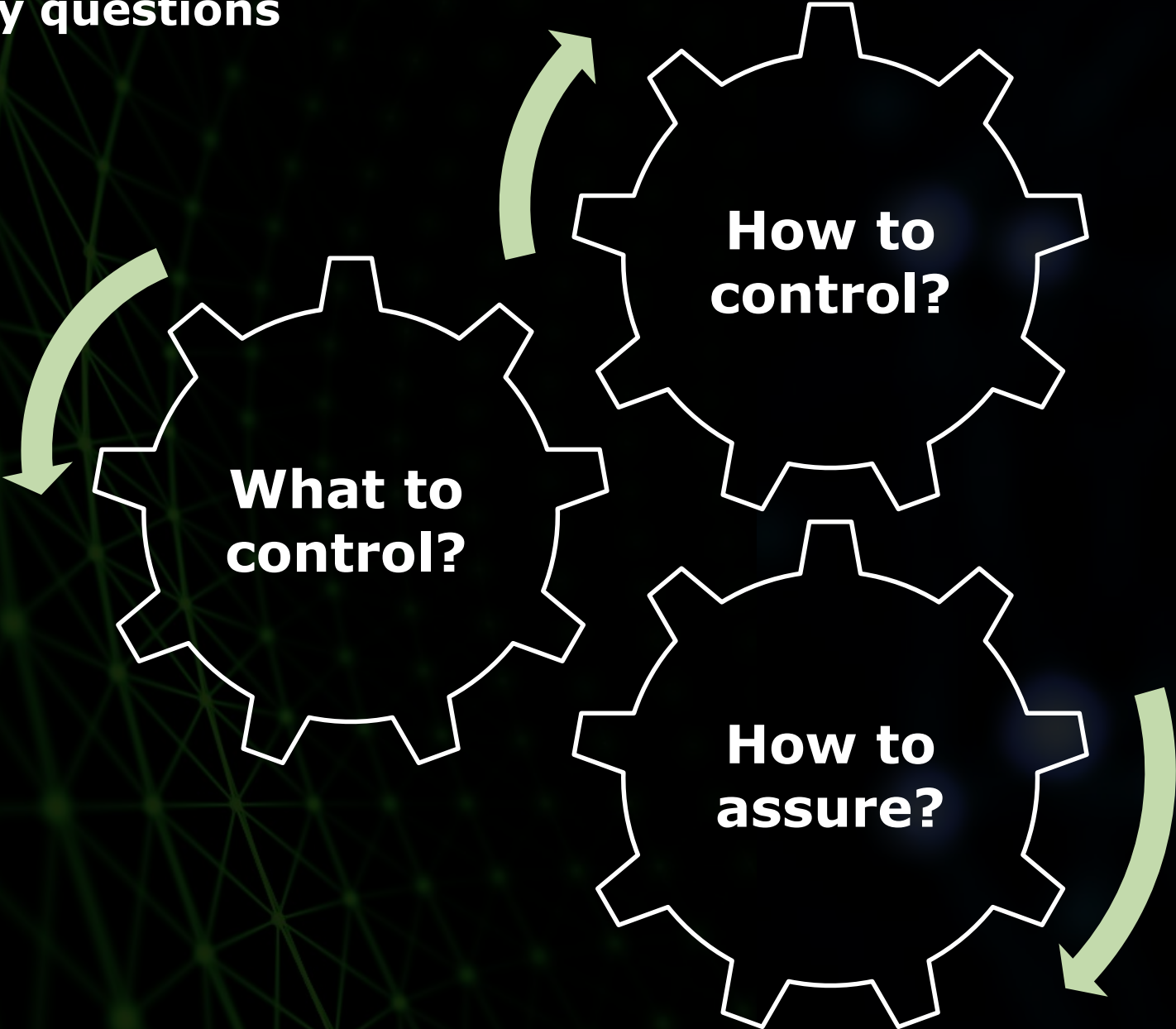
Limited utilisation of monitoring techniques ... no one version of truth

Lack of coherent approach to monitoring and testing

Limited leverage of technological or digital capabilities

Lack of positive controls culture

Three key questions



“The question is not **if** but **when** the new era of control automation will have its **full impact** on your organisation”

Example: Robotic Process Automation

Deloitte.



The future of controls
Robotic process automation

▶ 00:03 / 02:32

What we just saw:

- ✓ Logging into applications securely
 - ✓ Generating report based on pre-defined parameters
 - ✓ Screen grab and archiving
 - ✓ Reading and comparing data from different sources
 - ✓ Creating information reports
 - ✓ Identifying and prioritising exceptions
 - ✓ Creating notifications
-



Enabling **Technology**

Future of Controls Ecosystem

What to control

How to control

How to assure

Continuous Learning and Improvement

Automated Controls Quality Assurance

Risk Sensing to define Risk Appetite

Integrated GRC

Integrated Compliance Framework

Controls Automation

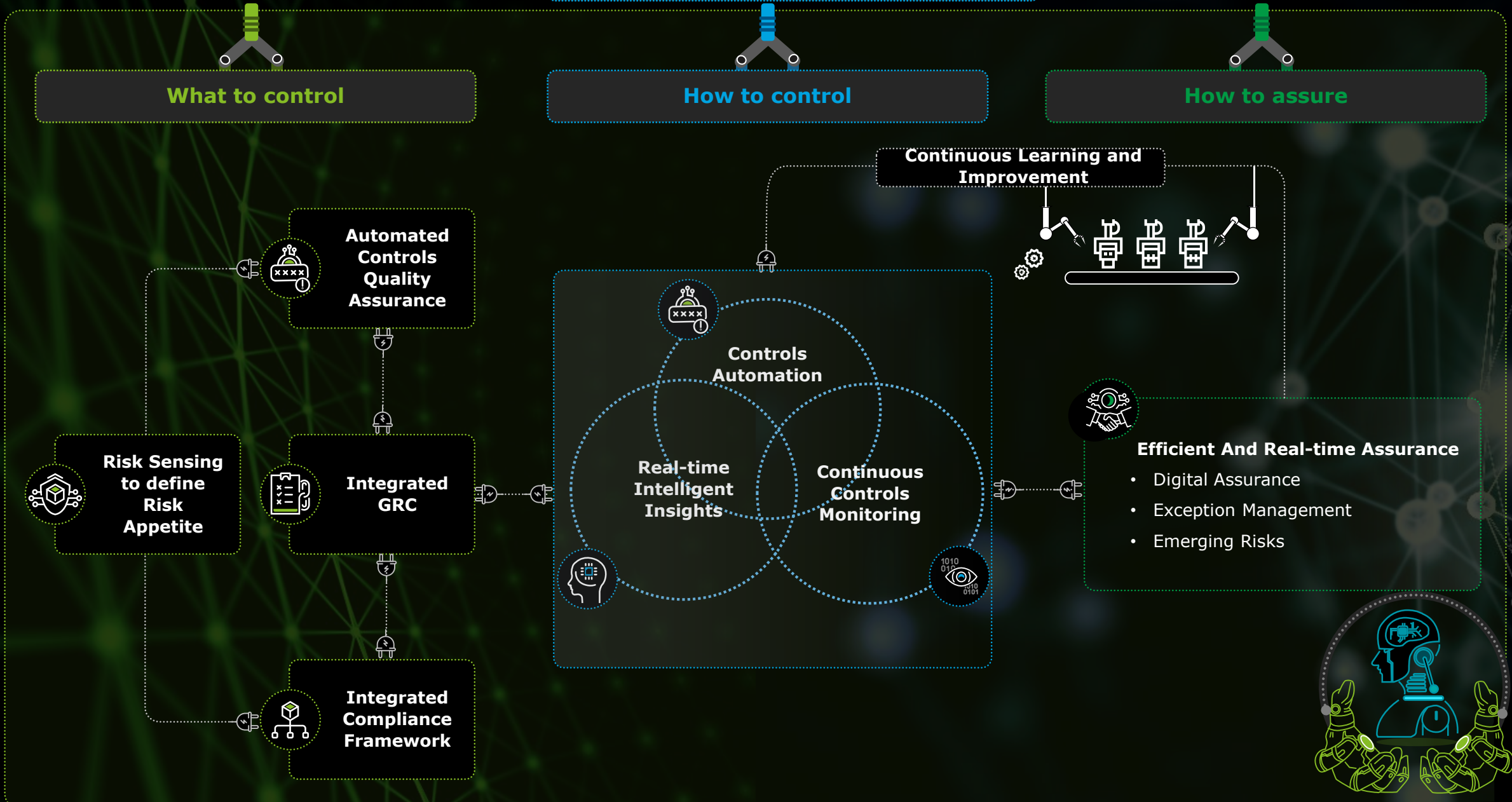
Real-time Intelligent Insights

Continuous Controls Monitoring

Efficient And Real-time Assurance

- Digital Assurance
- Exception Management
- Emerging Risks

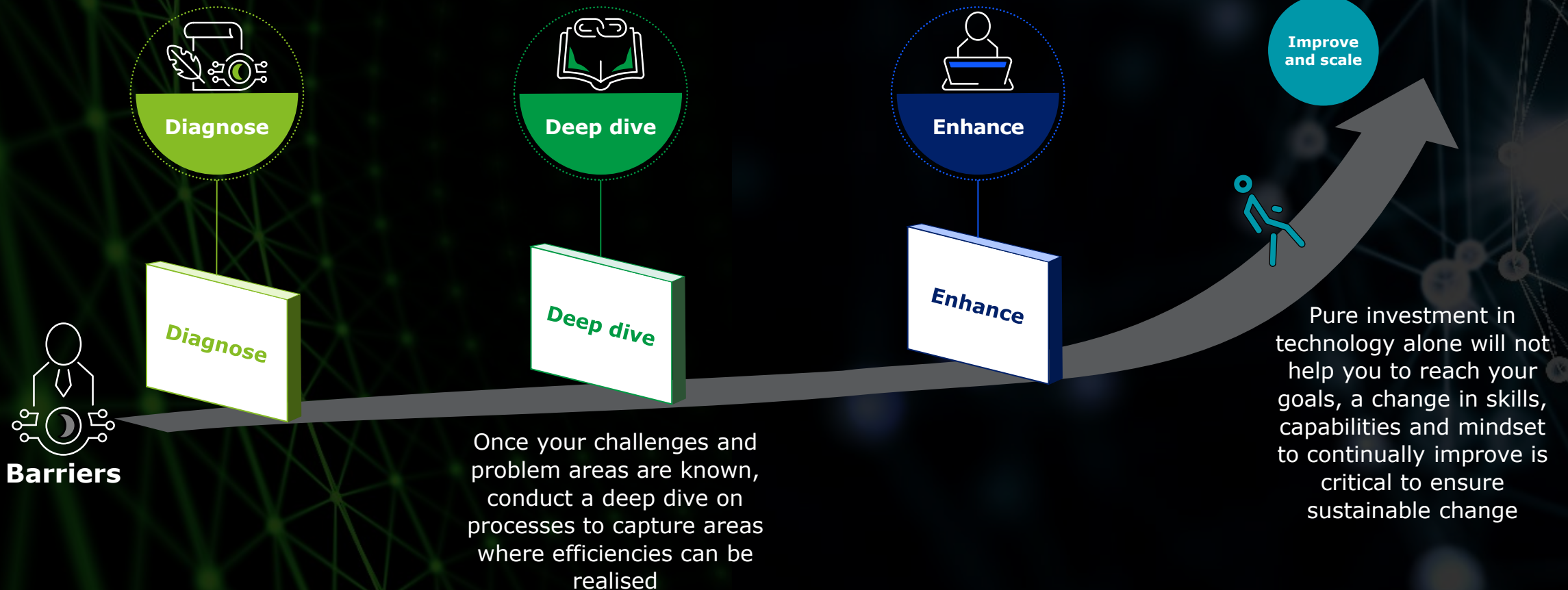
Culture



Future of controls – journey to enhancing your controls

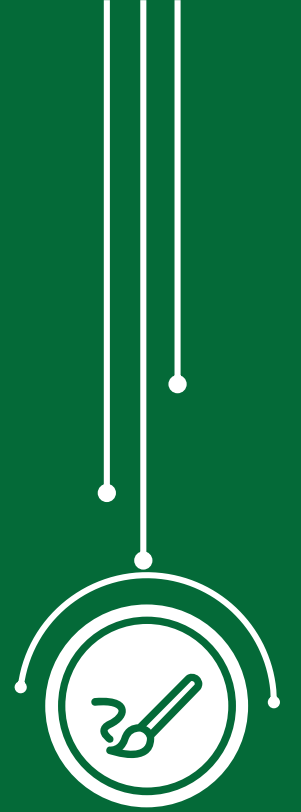
Start with understanding the problem and your control challenges. Define your mindset and appetite for change, together with the goals for enhancing your control framework

Leveraging the outputs from the previous sessions, explore the solutions, barriers to change and roadmap for implementation

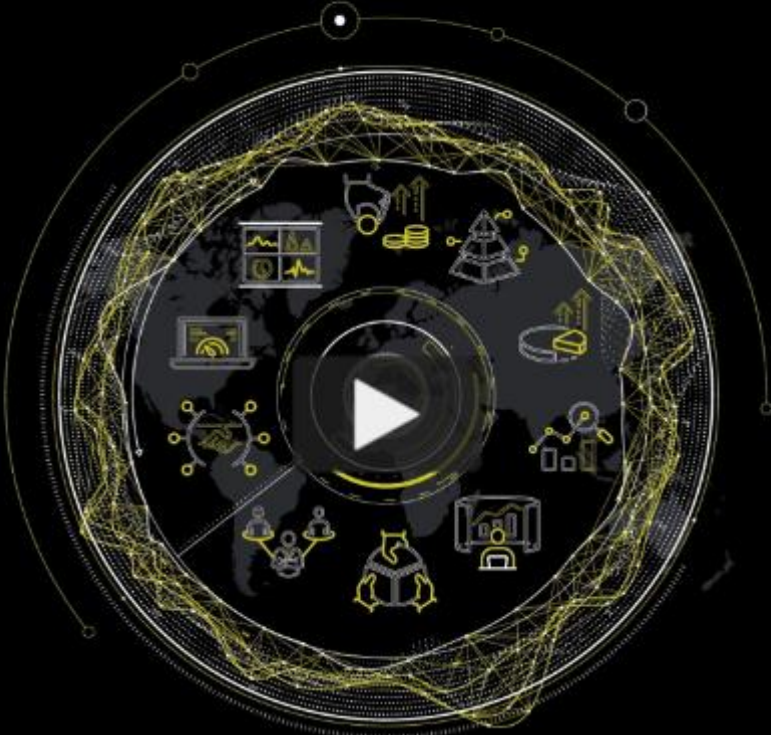


The Controls Hub

Ian Orgill



Deloitte.



Controls Hub

▶ 00:00 / 03:38 🔊 ↗

Deloitte.



Jon Thomson

E: jonthomson@deloitte.co.uk



Sonya Butters

E: sobutters@deloitte.co.uk



Michael Jones

E: mwjones@deloitte.co.uk



Anil Sen Gupta

E: ansengupta@deloitte.co.uk



Ian Orgil

E: iorgill@deloitte.co.uk



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2020 Deloitte LLP. All rights reserved.