Internal Auditors Committee (IAC) - Forum Event

Tuesday 17 July 15.00 - 16.30
Old Library - Lloyd's

Agenda

• Introduction	Gerald Dodds (IAC)
• Wooden Ships to Robotics – Where next For Internal Audit	Mike Taylor, President of the Chartered Institute of Internal Auditors
• Impact and issues for internal auditors arising from GDPR –	Stephen Hopkins, Deloitte
• Lloyd's update -	Peter Montanaro, Lloyd's
• Panel / Q&A session	

INSIGHT CONSENSUS INFLUENCE

Role of Internal Auditors Committee

Dialogue with Lloyd's

- engage with Lloyd's on IA matters and related policy
- provide practitioner feedback to Lloyd's (and others)

Community

- manage any IA forum events
- publicise and communicate any relevant information to IA staff working in the Lloyd's market e.g. NEDs views on Internal Audit
- reach out to other assurance providers within the LMA e.g. CRO Committee

Consider

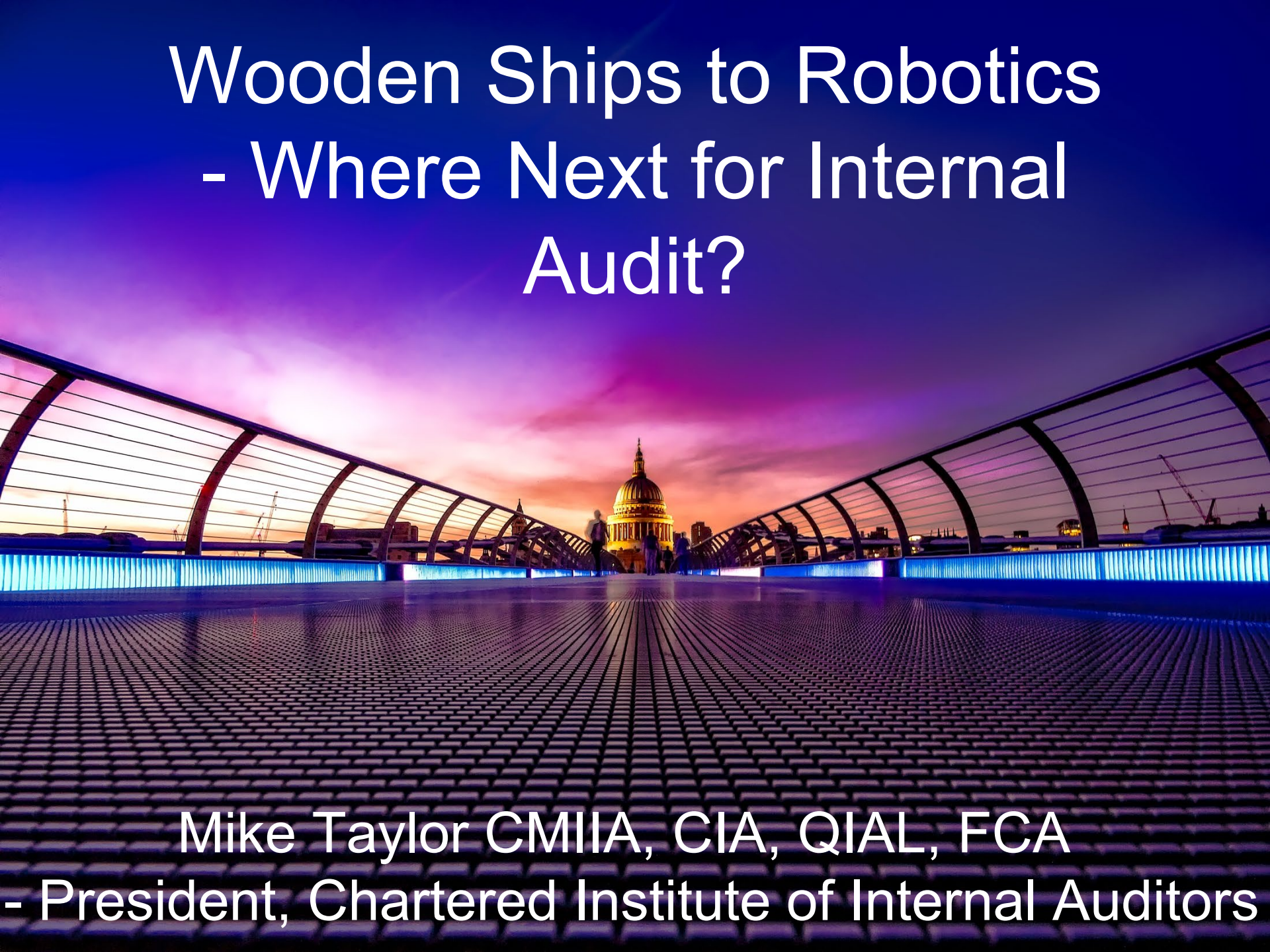
- changes to requirements / standards developed by Lloyd's, IIA, FCA, PRA, and others e.g. changes to the FS Code

Members of Internal Auditors Committee

- **Gerald Dodds, Chair – Canopius [gerald.dodds@canopius.com]**
- **David Kelly, Deputy Chair - Brit**
- **Gary Budinger , LMA Committee Secretary [Gary.Budinger@LMALloyds.com]**
- **Chris Hood, Hiscox**
- **Chris Khan, Lloyd's**
- **Elizabeth Bodnarova, Chaucer**
- **Ola Bello, ERS**
- **Anil Vaidya, Atrium**
- **Sharon Walker, XL Catlin**
- **Stephen Hartley, Cathedral**

Please contact us directly / reach out with your views on things that affect you

Wooden Ships to Robotics - Where Next for Internal Audit?



Mike Taylor CMIIA, CIA, QIAL, FCA
- President, Chartered Institute of Internal Auditors

From Wooden Ships…….

- Cyclical to risk based
- Samples to analytics
- Quantity to quality
- Finance to infinity
- Independence to objective
- Living dead to talent of the future
- ‘What is internal audit’ to ‘The last line of defence’
- ‘Internal Audit is dull’ to ‘#internalauditiscool’
- False dawns: CRSA, Continuous auditing….

Challenges

- Expectations
- Own goals - Financial crisis, Volkswagen, Carillion, Dixons Carphone….
- Emerging risks - Cyber, Brexit, Culture, New regulation, ??
- Skills gaps - Data Analytics, AI
- People - quality and quantity

Expectations

- Stakeholders reporting that internal audit adds significant value dropped from 54% in 2016 to only 44% in 2017
- 68% of board members and 77% of management believe internal audit's current level of involvement in disruptive events is not sufficient
- But 18% of respondents report that their internal audit function plays a valuable role in helping their companies anticipate and respond to business disruption
- In 2015 55% of respondents said they wanted internal audit to be a trusted advisor by 2020
- In 2017 just 9% consider internal audit a trusted advisor

2017 State of the Internal Audit Profession Study, PwC

Challenges

- Own goals - Financial crisis, Volkswagen, Carillion, Dixons Carphone….
- Emerging risks - Cyber / Privacy (GDPR), Brexit, Culture, New regulation, Speed of Change, ??
- Skills gaps - Cyber, Data Analytics, AI
- People - quality and quantity

….to Robotics

- Professionalism
- Corporate Governance Code
- Applying the refreshed FS Code
- Advanced data analytics
- Cyber auditing
- Agile Auditing
- Augmented intelligence
- Continued developments around values and culture
- Internal audit as talent hub

Your Institute

Refreshed CIIA Vision

Professional internal audit will be recognised as essential to the success of organisations ***and their leaders*** and…

…the Institute will be recognised as ***essential*** to the ***success*** of internal audit professionals.

Your Institute

- Stakeholder engagement - PRA, FCA, FRC, IoD, Boards
- Effective Internal Audit Code(s)
- Corporate Governance Code update
- Risk in Focus
- New CIIA strategy implementation - Leaders Forum, Audit Leaders, Aspire, WIIA, Knowledge Factory, digitalisation…

Thank You

Deloitte.

Lloyd's Market Association
Internal Audit Committee
GDPR – Impact and Issues for Internal Audit

July 2018 | Stephen Hopkins, Director, Cyber Risk and Privacy Services

Contents

Introduction

The GDPR has some significant differences from the DPA

Whilst the GDPR is built upon similar foundations to the DPA, the intention was to be disruptive to force a greater focus on the protection of personal data:

- Strict sanctions regime – 4% Global Turnover / €20m
- Strong focus on Accountability
- Requirement for a Data Protection Officer
- Data Breach Reporting
- Consent must be freely given and unambiguous
- There are more Individual Subject Rights and less time to action them
- Data Protection by Design
- Maintain (and report upon) Records of Processing

GDPR compliance isn't a case of "once and done"

- The authors of the GDPR didn't want the Regulation to be treated as a 'tick box' exercise.
- Remaining compliant with the GDPR means embedding key data-protection processes into your Business As Usual operations.
- Being able to find evidence that key processes have been adopted and are being used, maintained and sustain will become an important area of focus for Internal Audit.

Many GDPR Programmes are still ongoing

- Whilst Many firms structured their GDPR programmes to deliver against a set of prioritised requirements by May 25th 2018, for many the work is still ongoing.
- Lower priority, or high-priority but complex areas of remediation remain outstanding.
- Common areas include of ongoing work include:
    - 3rd Party Contract Amendment
    - Unstructured Data
    - Systems Remediation

Areas of focus for Internal Audit

Help identify whether GDPR compliance is part of the company's

GDPR subject area	Rationale	Key questions
Accountability	Foundational component within the GDPR and expected to be a focus for the UK Regulator.	• How are data protection roles and responsibilities being communicated, accepted and executed? • What evidence is there that data protection activities are being executed?
DPO / DPO Function	New functions, often in transition to a target state operating model, which require support from across the business to be effective.	• How has the role and activities of the DPO been communicated? • Does the DPO have sufficient authority? • Do we have any headcount / skills issues?
Data Retention	Over-retention of data has been an ongoing problem.	• How are we ensuring that our data retention rules are being applied by business owners? • How are we confident that our data retention periods are defensible?
Reporting	Reporting on the effectiveness of data protection needs to be in place and working properly.	• How are we going about answering the question of "Are we GDPR compliant?" • What data are we collecting to support our view of the company's level of compliance?
Individual Subject Rights	Need to address these effectively or else risk complaints.	• What are we doing to ensure we can meet mandated timeframes? • How do we know if a request for data erasure can be rejected or not?
Consent and Transparency	Very easy for customers and regulators to see if you're getting these wrong.	• Where and why are we using Consent? • Who has oversight of our consent management processes and transparency wordings? • What information are we capturing when consent is given?
Records of Processing	Fundamental capability that underpins GDPR compliance.	• How are we ensuring that our records of processing is kept up-to-date? • How have we proven our reporting capability?
Breach Management	New reporting requirements need to be underpinned by consistent, reliable breach management processes.	• How are we ensuring consistent breach classification? • How are we confident that we can meet the 72 hour deadline?
Privacy by Design	Fundamental requirement that privacy impacts of new systems and processes are considered	• How do we know that our privacy impact assessment processes are effective? • How are we capturing privacy impacts of non-project spend?

Conclusions

Help the DPO understand what is (and isn't) going

- In most organisations, it is the DPO who will be asked the question, "Are we GDPR compliant?"
- Internal Audit has an important role to play in helping the DPO answer that question – especially as the DPO function is often quite new and is still working on achieving a target state and building its operational capability – by reviewing the effectiveness of GDPR-aligned operational activities.

Identify which GDPR-related practices have (and haven't) been

- Formulate an Audit schedule that focusses on GDPR-related "embedding reviews".
- Use the embedding reviews to ascertain whether the organisation is doing the right things, in relation to the embedding and sustaining of GDPR-related activities.
- Focus on those items that are substantially new to the organisation and / or are likely to result in customer complaints if they are done poorly.

Keep a watchful eye on any ongoing GDPR programmes or

- Understand what GDPR-related projects or programmes continue to run:
  - How are they maintaining traceability back to a known gap or set of gaps?
  - How are they ensuring that they have the 'right' solutions?
  - What is their planned completion date and are they on track to deliver?

Deloitte.

Important notice

This document has been prepared by Deloitte LLP for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of Deloitte LLP to supply the proposed services.

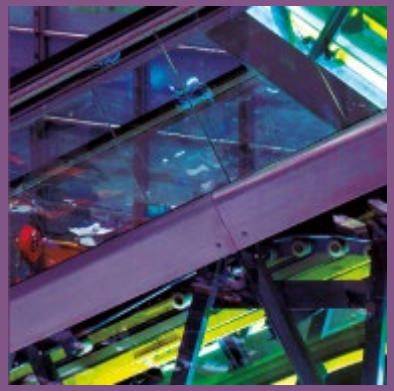
The information contained in this document has been compiled by Deloitte LLP and may include material obtained from various sources which have not been verified or audited. This document also contains material proprietary to Deloitte LLP. Except in the general context of evaluating the capabilities of Deloitte LLP, no reliance may be placed for any purposes whatsoever on the contents of this document. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Deloitte LLP or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document.

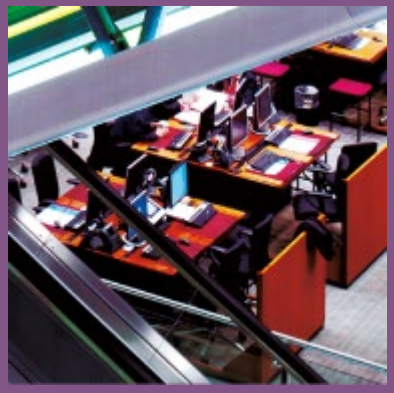
Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London, EC4A 3BZ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE 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 NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

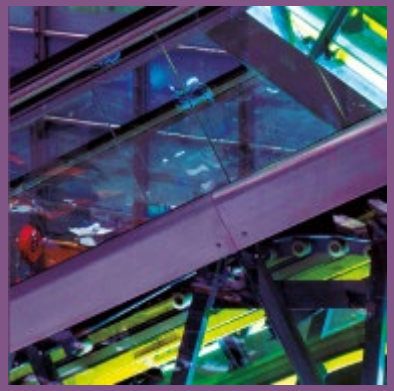


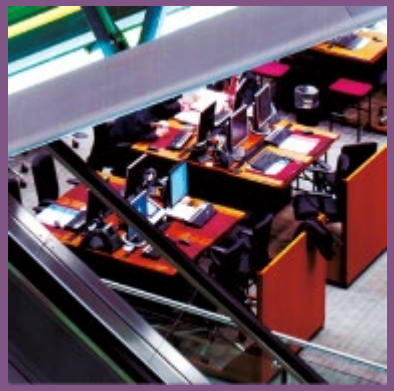


Lloyd's Update
Peter Montanaro

Head of Syndicate Capability Oversight
Lloyd's Performance Management Directorate

INSIGHT CONSENSUS INFLUENCE





Panel Discussion/Q & A

http://www.lmalloyds.com

INSIGHT CONSENSUS INFLUENCE