LLOYD'S

Lloyd's Coverholder Auditors Conference

"Remaining relevant in a changing world"

Objectives for the Conference

Paul Brady, Head of Policyholder & Third Party Oversight

Lloyd’s

Auditors' Conference 2019

Agenda

"Remaining Relevant in a Changing World"

8.30 Registration and coffee

9.00 Welcome and Market Conditions update, *Jon Hancock, Lloyd's*

9.30 Objectives for the Conference, *Paul Brady, Lloyd's*

9.40 DA Initiatives, *Lindsey Davies, Lloyd's*

10.00 The AiMS journey, *Ben Thomas, Lloyd's*

10.30 Audit efficiency – Coordination, *Leena Ekman, Lloyd's*

10.50 Coffee break

11.10 Thematic Reviews update, *Jenny Neale, Lloyd's*

11.30 Audit scoping exercise and feedback – What does risk-based scoping look like?
Leena Ekman & Kate Czamara-Newton, Lloyd's

13.00 Lunch and networking

A

Auditors’ Conference 2019
Agenda

14.00 Auditor Accreditation - *Paul Brady, Lloyd’s, Mark Taylor, Turnstone & Nick Barnaby, Lloyd’s*
14.30 TPA Audits - *Scott Kellers, Liberty & Lorraine Calway, Goldseal*
15.00 Cyber Security - *Peter Montanaro, Mo Philip & Nick Barnaby/Lloyd’s*

15.30 Coffee break
15.50 DAG Update - *Tom Hamill, LMA, Peter Bolster, MS Amlin & Stuart Johnson, AxaXL*
16.10 Q&A Panel based on Slido questions - *Speakers*
17.00 Wrap up & Close – *Paul Brady, Lloyd’s*

17.30 Drinks *at the Minories Pub, 64-73 Minories. London EC3N 1JL*

NB: Slido will be used throughout the day

DA Initiatives

Lindsey Davies, Senior Manager

Lloyd’s

Current Delegated Authority

Duplicated effort

Inconsistent, low-quality data

Barriers to entry for new DA business

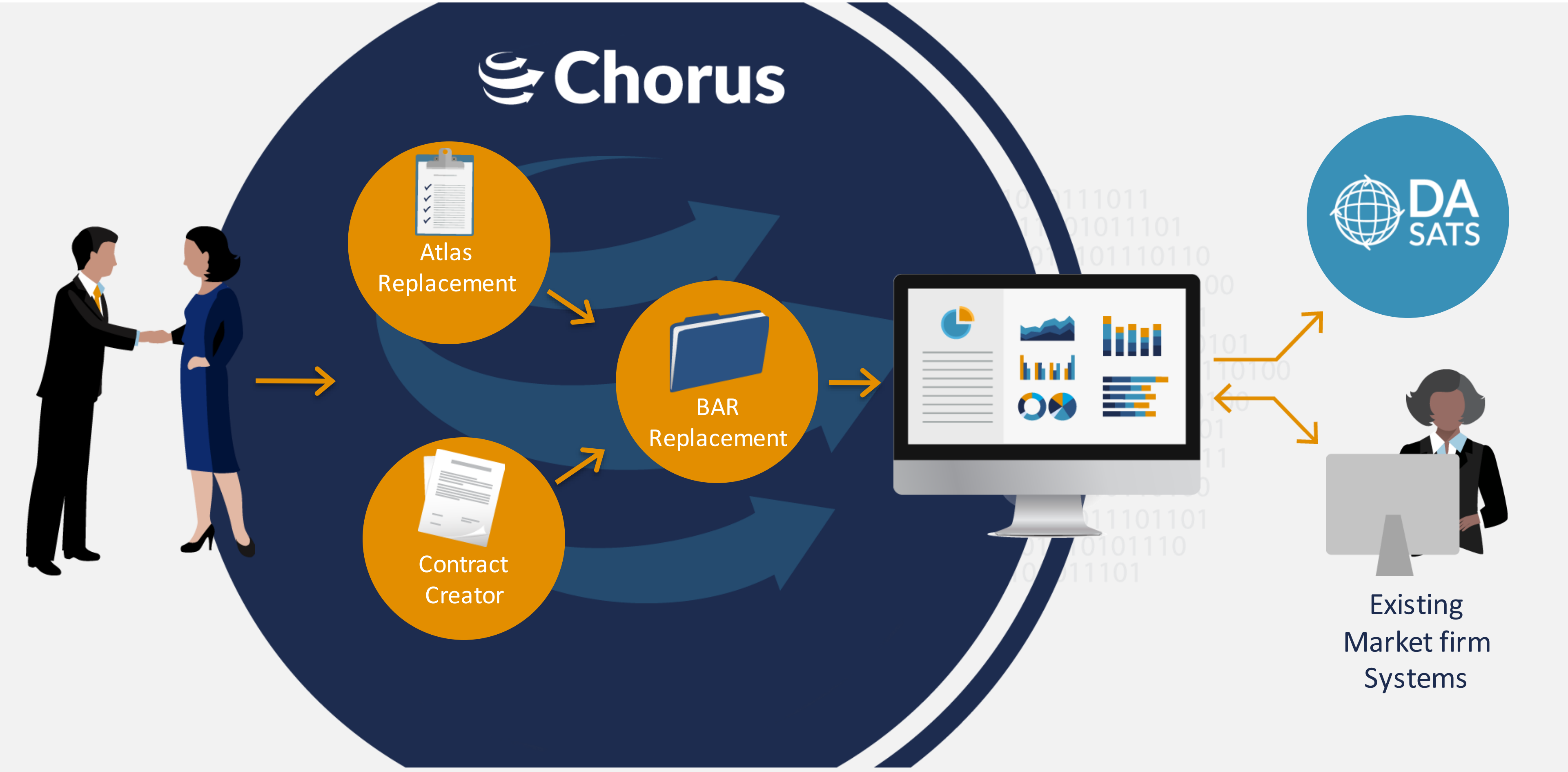
Future Delegated Authority

Less re-keying

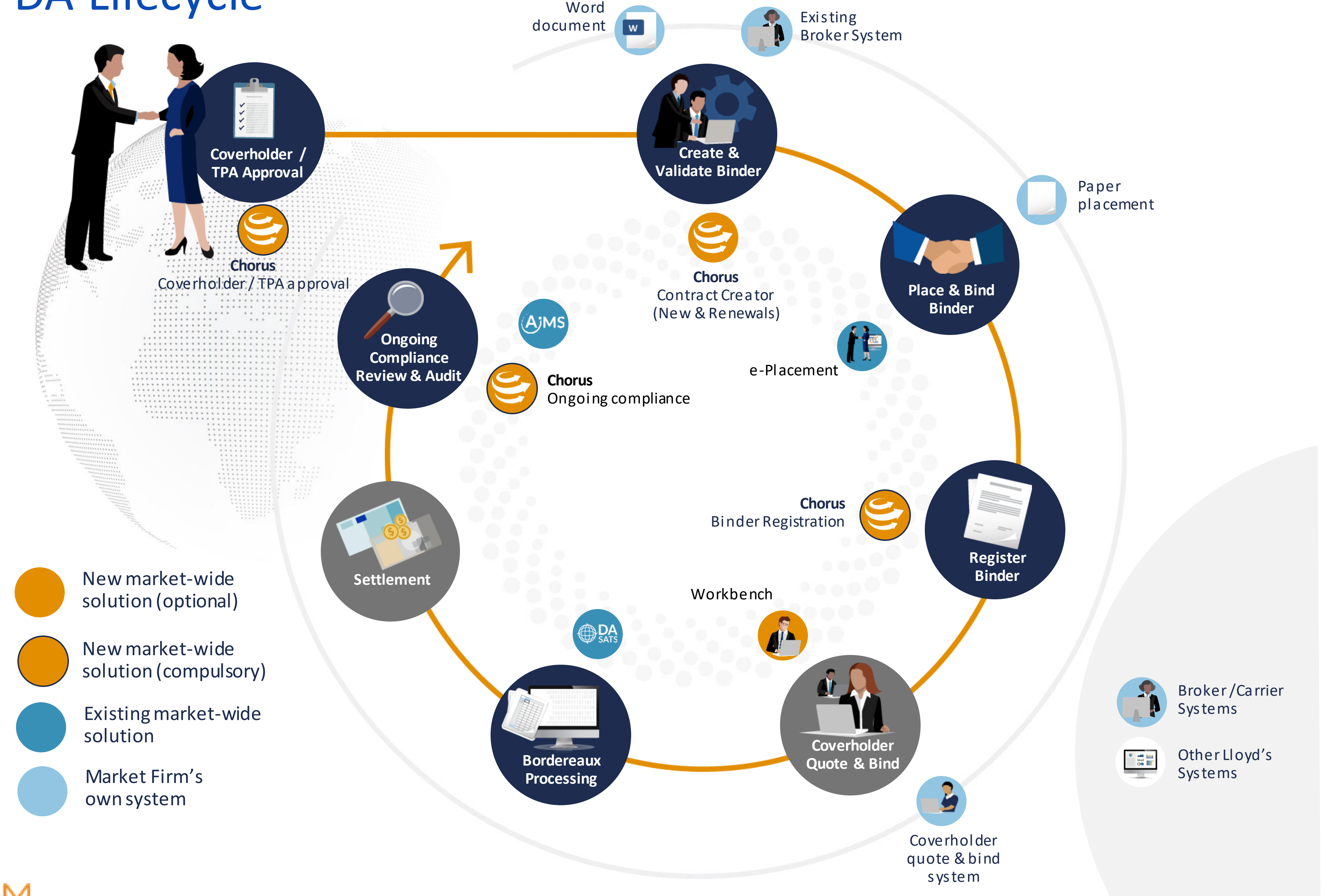
Consistent, validated data

Easier access for new DA business

Chorus - A new platform developed by the LM TOM



DA Lifecycle



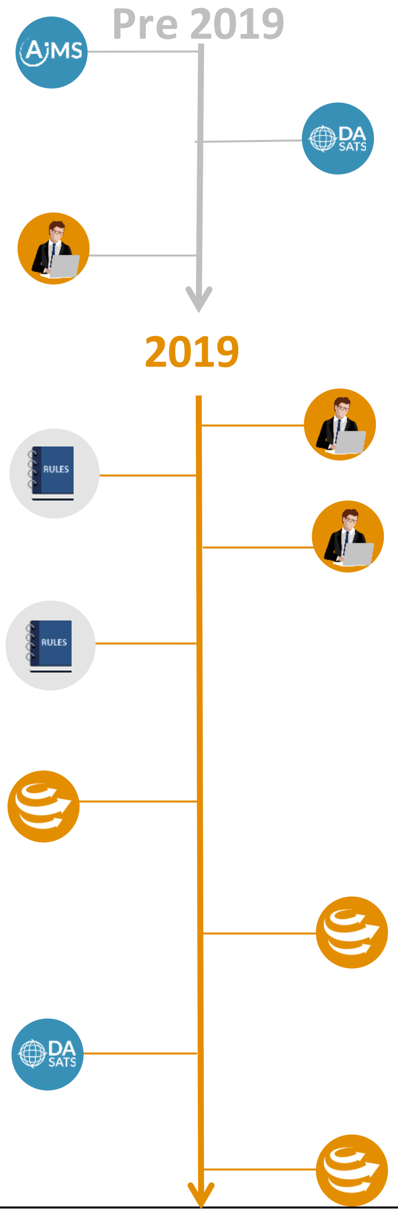
● New market-wide solution (optional)

● New market-wide solution (compulsory)

● Existing market-wide solution

● Market Firm's own system

Classification: Confidential



Pre 2019

AiMS Go-live
October 2017

DA SATS Go-live
August 2018

Workbench pilot successfully completed
December 2018

2019

Workbench engagement continues
January – April

Workbench wider rollout begins
April

Lloyd's Byelaw change response required (subject to consultation)
April

Chorus MAT
Q1

Chorus Market Engagement
Q1 onwards

DA SATS next release
Q2

Chorus Go-live
Q3 2019

Where to go for more information

Third Party Byelaw Consultation
Visit Lloyds.com

Chorus
Visit tomsupports.london
Email LMTOMDA@lmtom.london

DA SATS
Visit tomsupports.london

Workbench
Visit lloyds.com/workbench
Email coverholderworkbench@lloyds.com

AiMS
Visit lloyds.com

Speak to your Association

- For information on how to get involved
- With DA questions
- To give feedback
- If you would like to be involved in MAT

Change Management support

We can provide change management support with our dedicated change team

Visit tomsupports.london

LLOYD'S

The AiMS journey

Ben Thomas, Manager

Lloyd’s

INNOVATION

EVOLUTION

INVENTION

DIGITALISATION

MODERNISATION

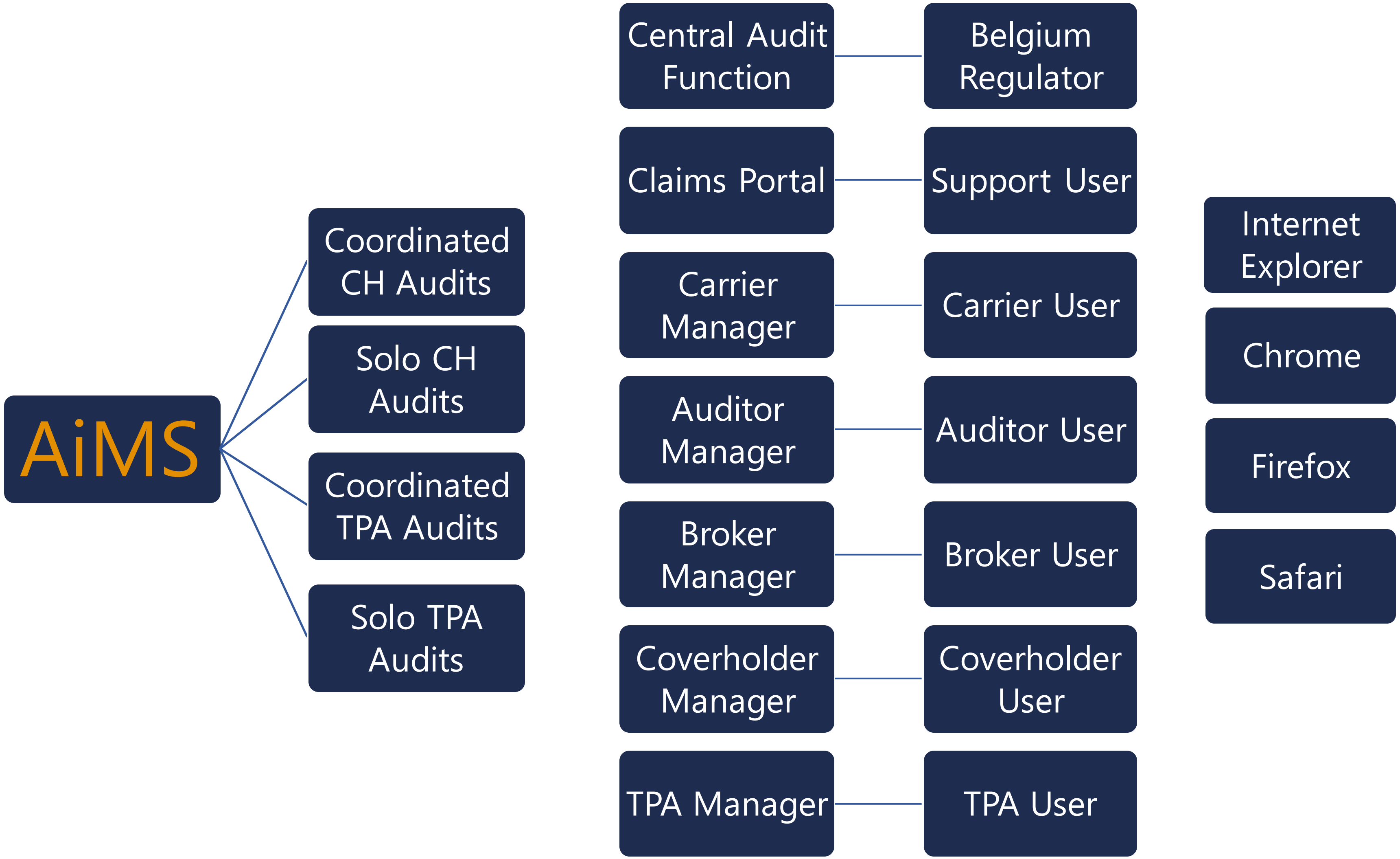
AIMS

Audit Information
Management System

AiMS

Audit Information Management System

AiMS 2.0



AiMS

Coordinated CH Audits

Solo CH Audits

Coordinated TPA Audits

Solo TPA Audits

Central Audit Function — Belgium Regulator

Claims Portal — Support User

Carrier Manager — Carrier User

Auditor Manager — Auditor User

Broker Manager — Broker User

Coverholder Manager — Coverholder User

TPA Manager — TPA User

Internet Explorer

Chrome

Firefox

Safari

51,000
Rules

200,000
Lines of Code

345
Unique System Generated Emails

13.3 million
Read Operations

6,500
System Users

27,000
Total Cases Generated

93,550
Test Scripts

3.5 Hrs
?

458
Change Requests

53
Road Map

73
Bug Fixes

763
Scoping Documents

8043
Recommendations

1617
Audit Reports

1376
Invoices

403
Solo Audits

AiMS

Audit Information
Management System

User Journey

2019

Road Map

Performance

LLOYD'S

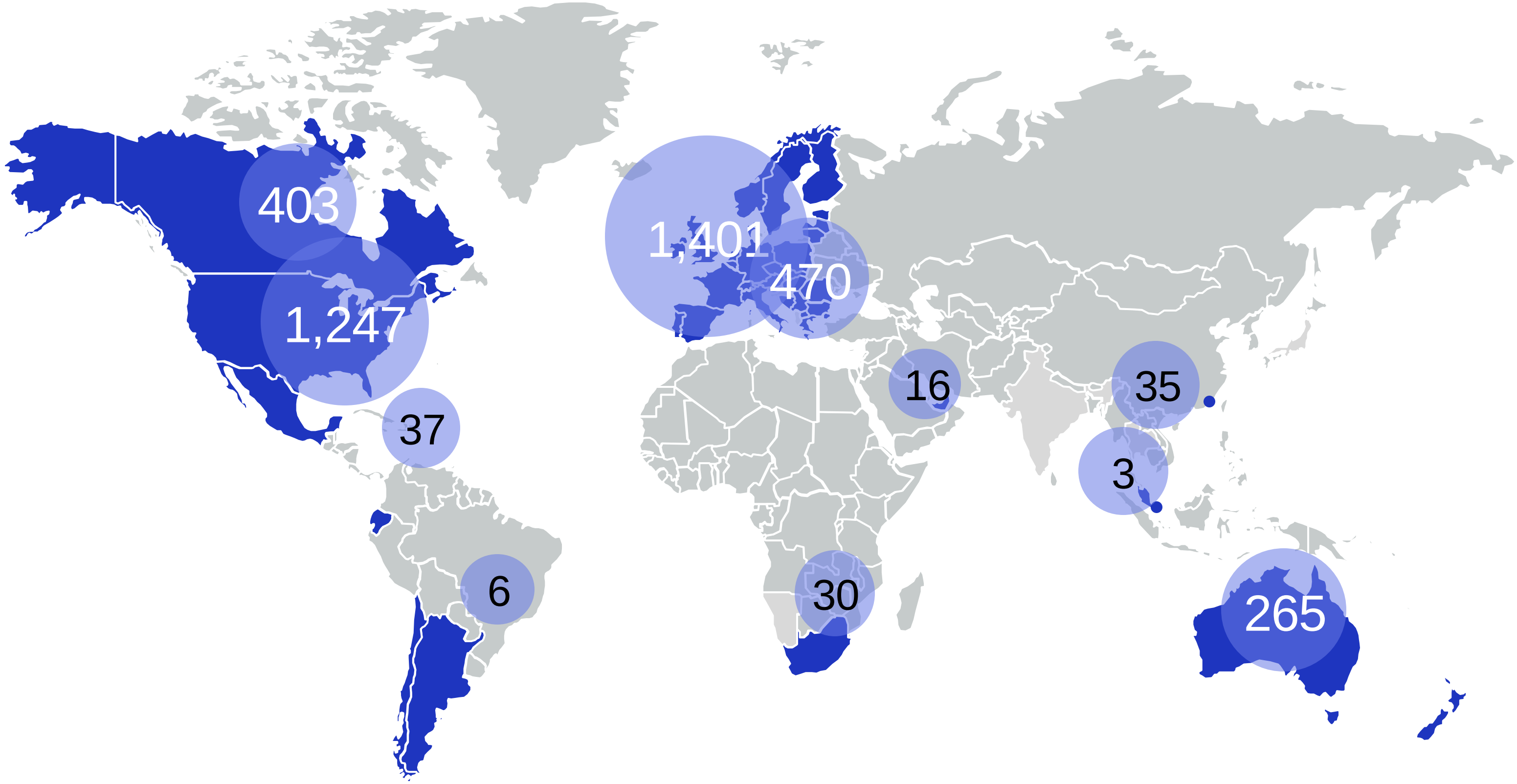
Audit efficiency – Coordination progress

Leena Ekman, Senior Manager

Lloyd’s

Coverholder business brings £10.4bn premium to the Lloyd's Market

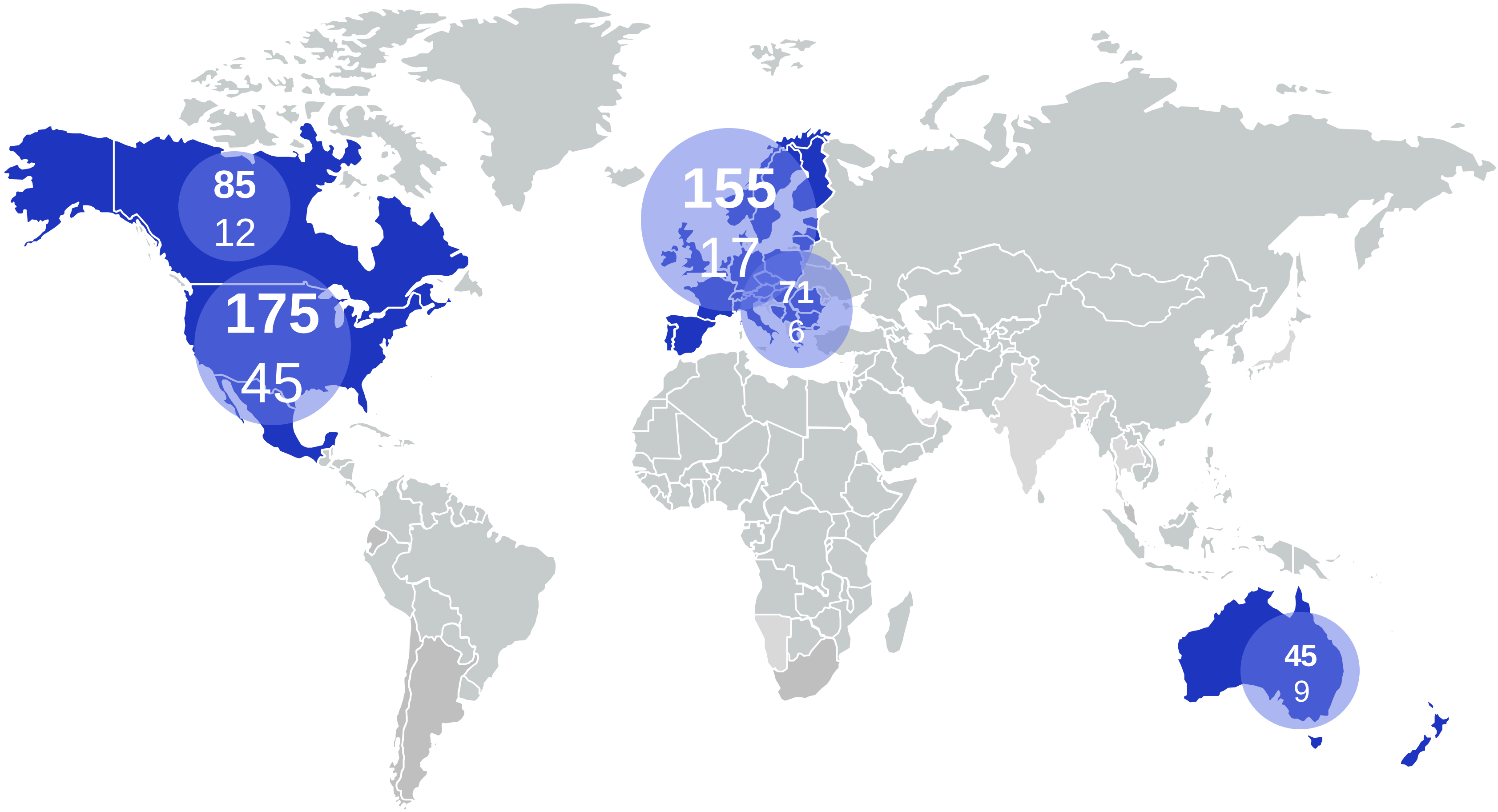
There are 3,936 approved coverholder office locations



Source: Lloyd's DA Dashboard – 31/01/2019

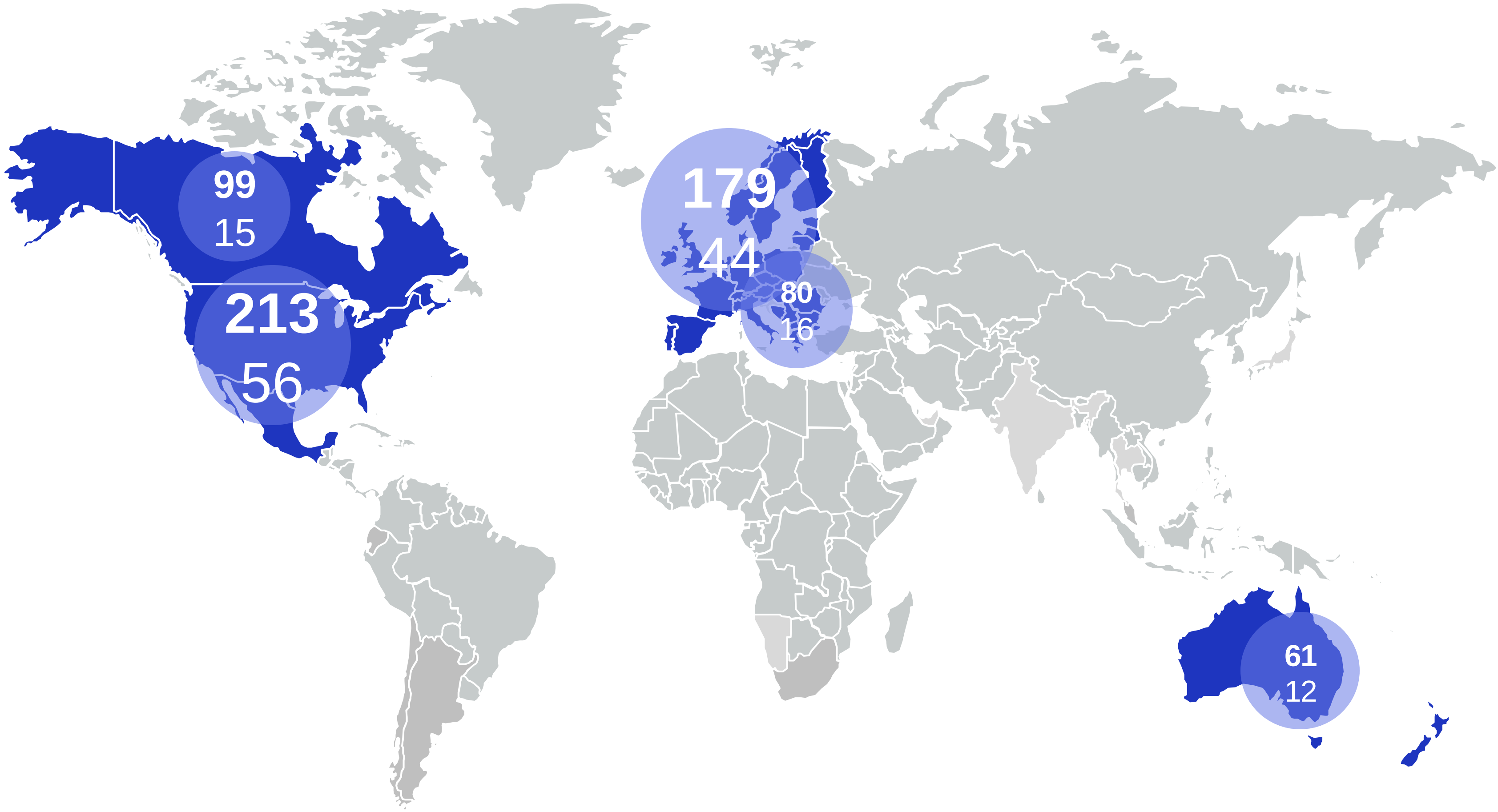
Coordinated audits 2018

550 coordinated coverholder audits covering 1,500 relationships and 1,800 UMRs, 39 auditors
90 coordinated TPA audits covering 240 relationships, 24 auditors



Coordinated audits 2019

640 coordinated coverholder audits covering 2,000 relationships and 3,000 UMRs, 36 auditors
150 coordinated TPA audits covering 560 relationships, 30 auditors

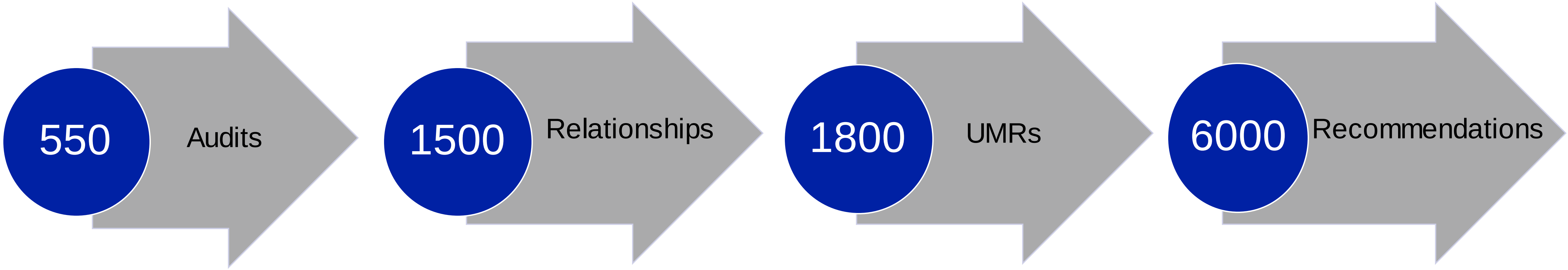


Key Priorities for 2019

- Continuous improvement and market support for AiMS to ensure full market adoption
- Continue TPA coordinated pilot through 2019 for full implementation in 2020
- Ensure adoption of New Risk Based Audit Scope for both Coverholder and TPA audits
- Improve scoping especially for large coordinated audits
- Utilise available MI for proactive rather than reactive 3rd Party management and oversight
- Initiate Auditor Accreditation process

Analysis of Findings & Recommendations

2018 Coverholder Audit Recommendations



550 Audits

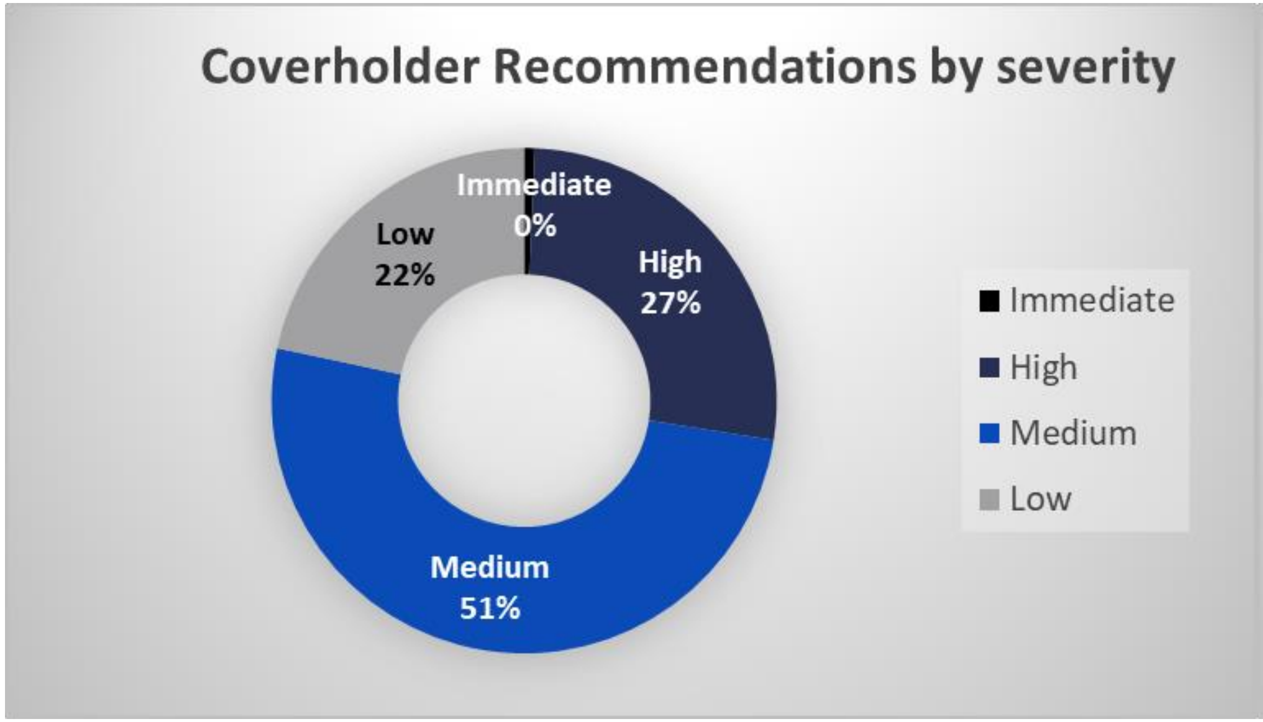
1500 Relationships

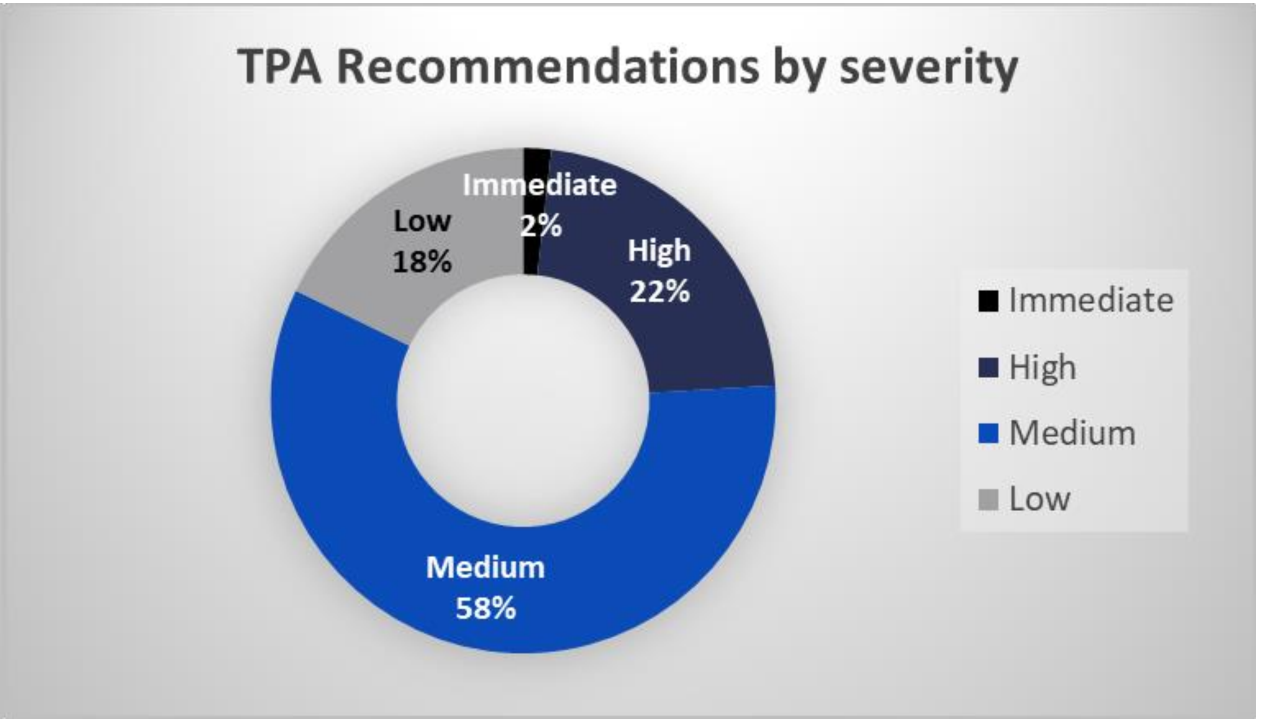
1800 UMRs

6000 Recommendations

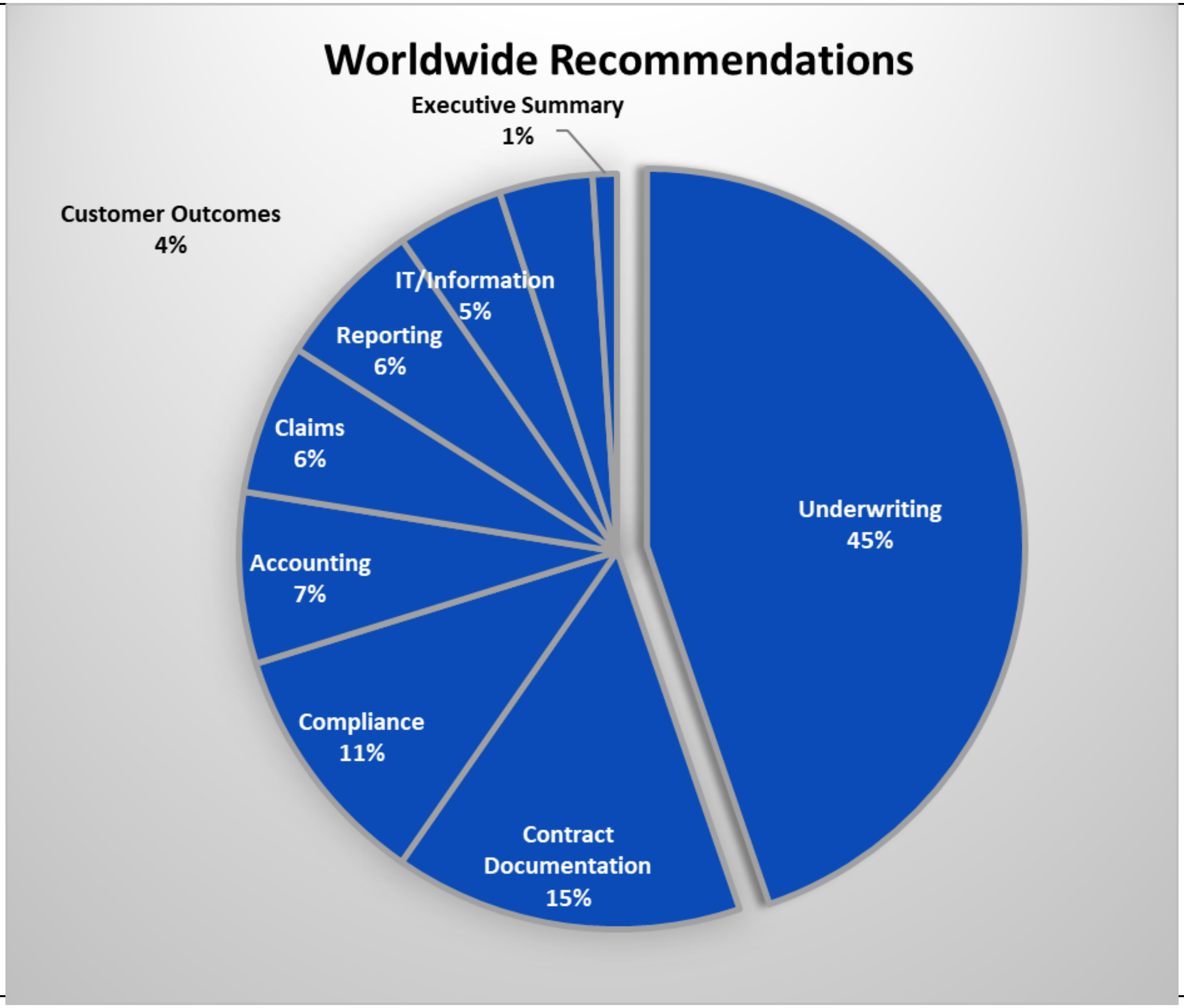
LLOYD'S

Split of recommendations by severity

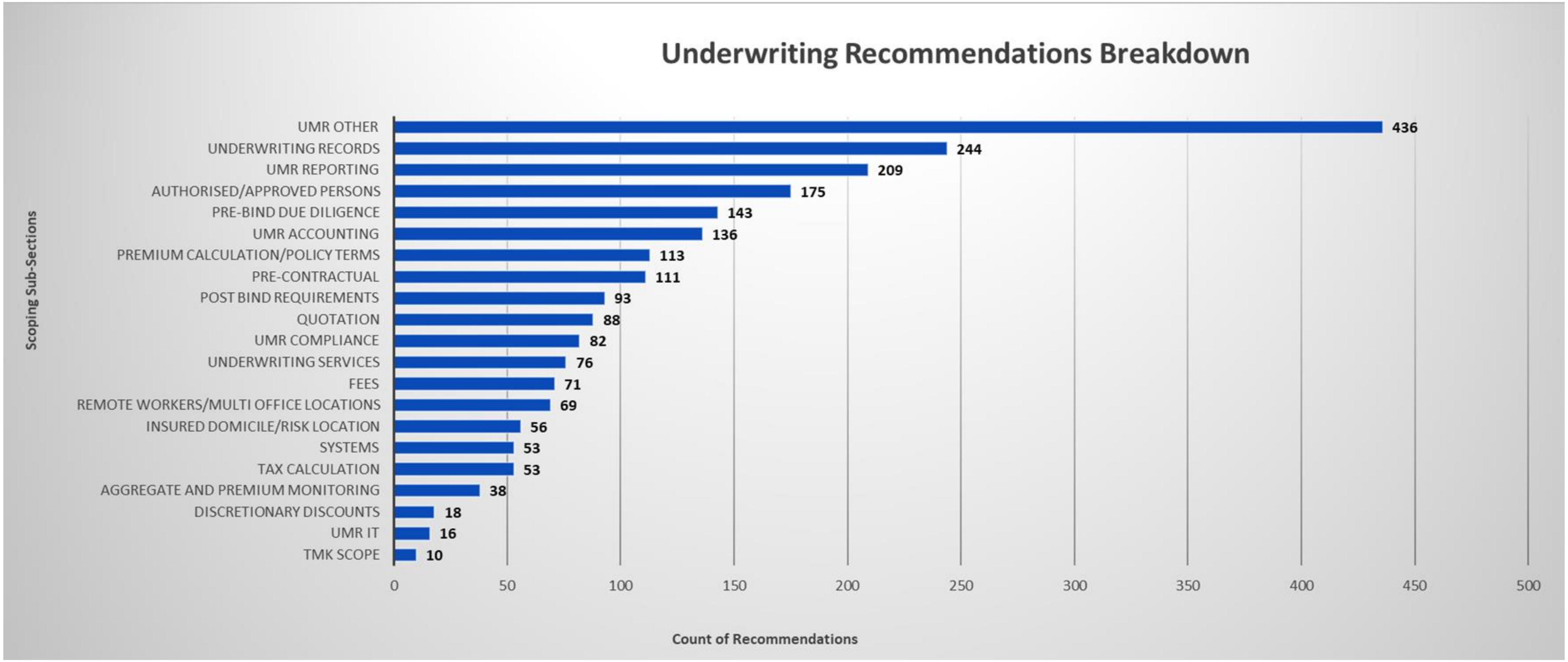




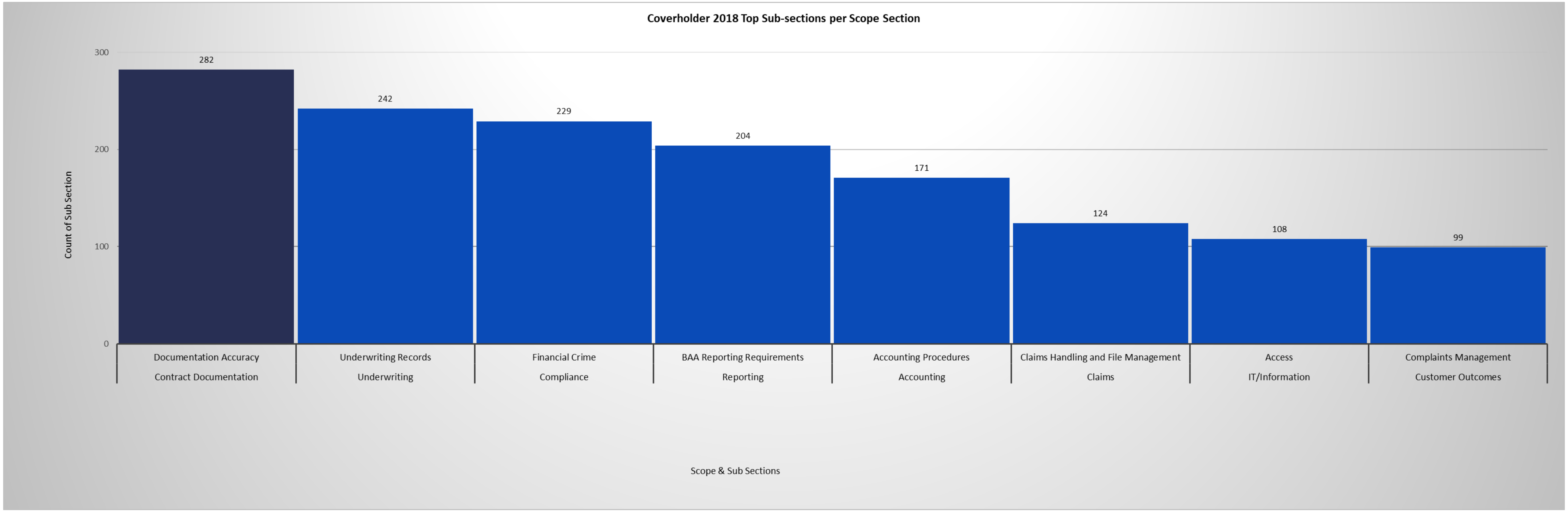
CH 2018 Findings & Recommendations by scope section



CH 2018 Underwriting Recommendations

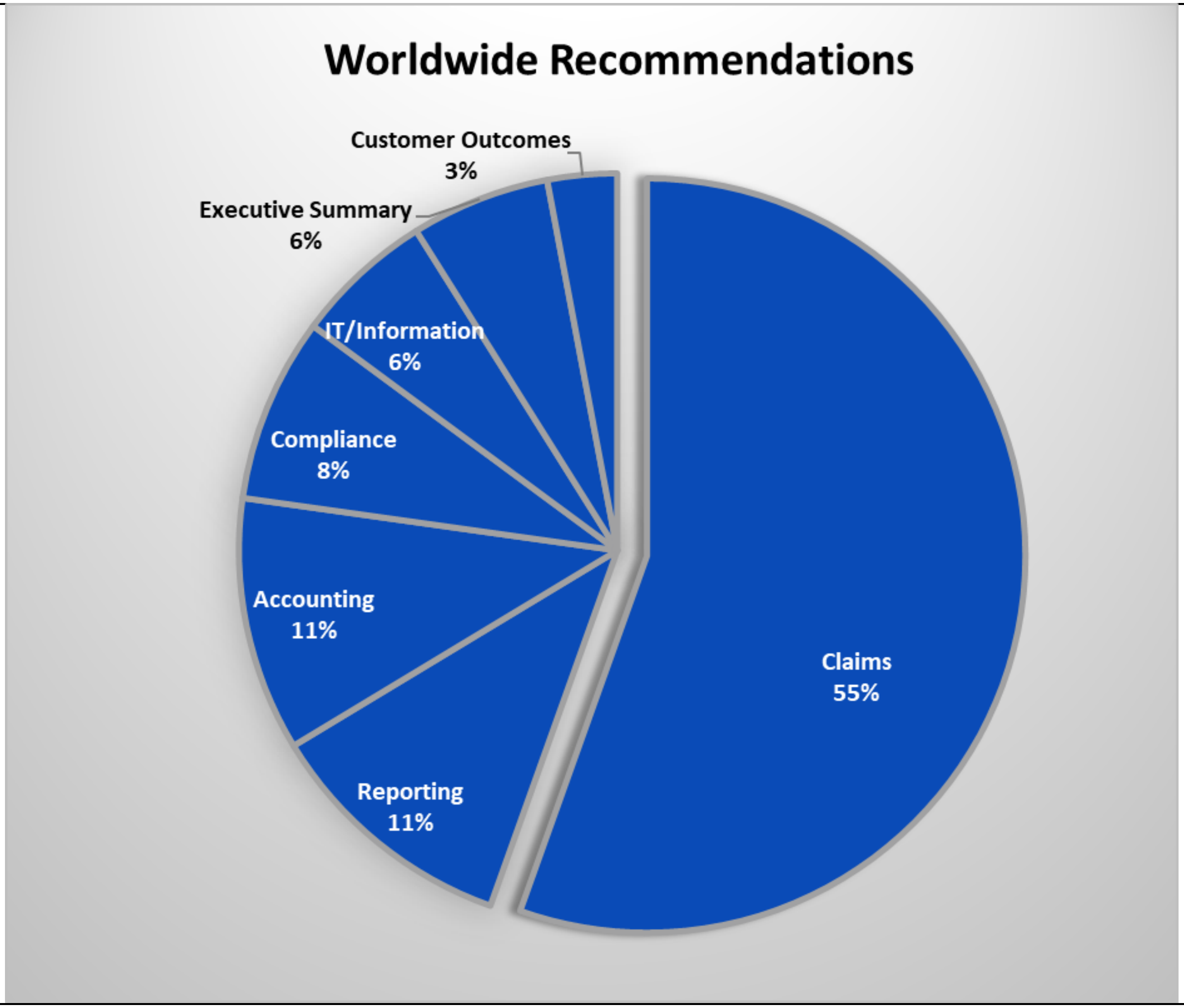


Coverholder 2018 Top Risks per Scope Section

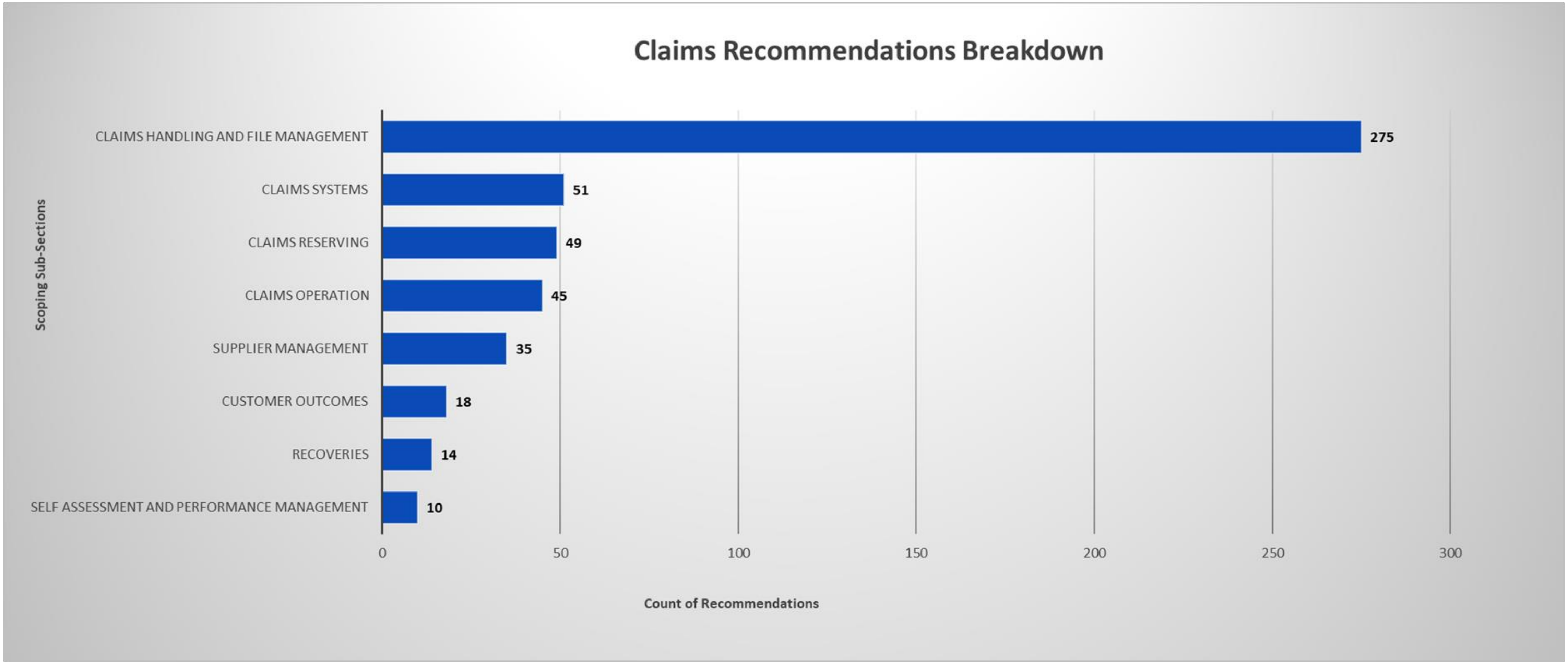


Classification: Confidential

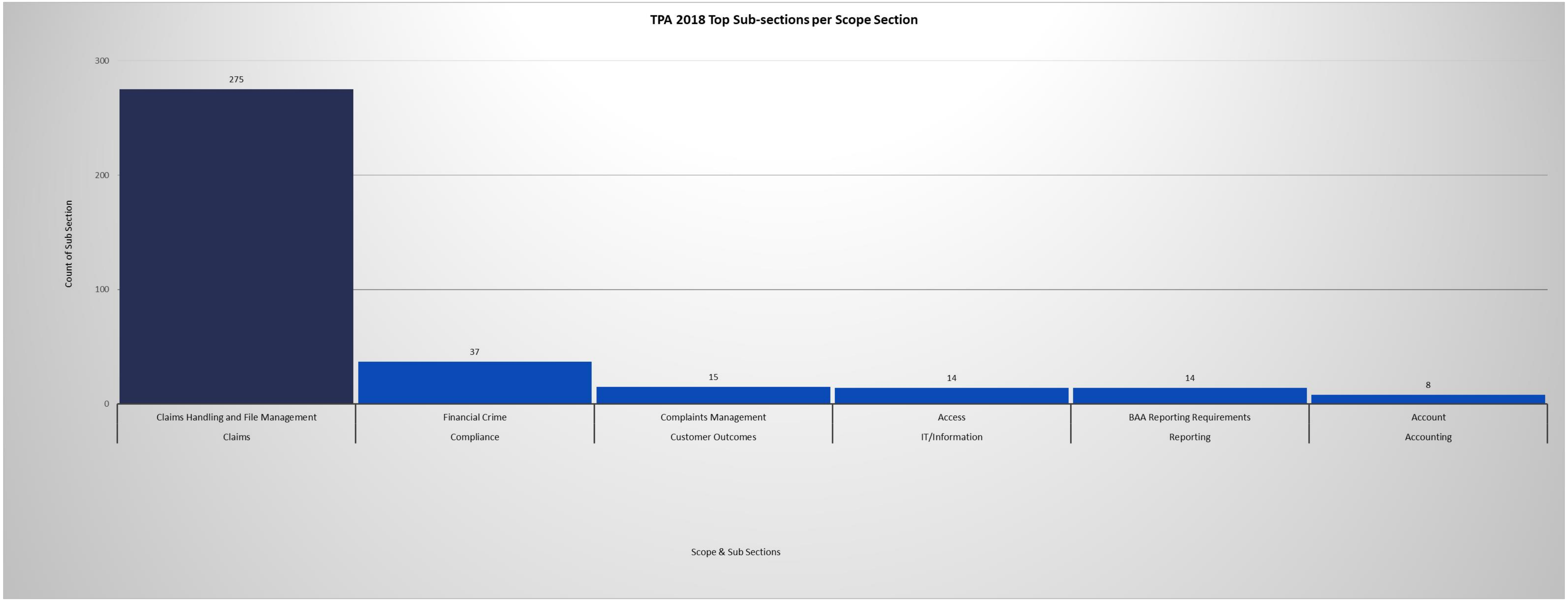
TPA 2018 Findings & Recommendations by scope section



TPA 2018 Claims Recommendations



TPA 2018 Top Risks per Scope Section



What next?

- Utilise available MI for proactive rather than reactive 3rd Party management and oversight

- Develop dashboards for all stakeholders

- Trend analysis of key issues and risks by scope section, territory class of business etc

- Work with the market to manage and mitigate risks pre-emptively to prevent them before they become potential problems

- Rating of coverholders by number/severity/ repeat recommendations etc as part of annual review process

Coffee break

LLOYD'S

Thematic Review update

Jenny Neale, Manager

Lloyd's

2018 Thematic Reviews

- Distribution of Consumer Products Through Master Policies
- Distribution of Storage & Removal Products
- Line slips & Consortia
- Acquisition Costs – Managing Agents Governance & Controls
- **Effective Use of Peer Review in Overseeing Delegated Authority Arrangements**

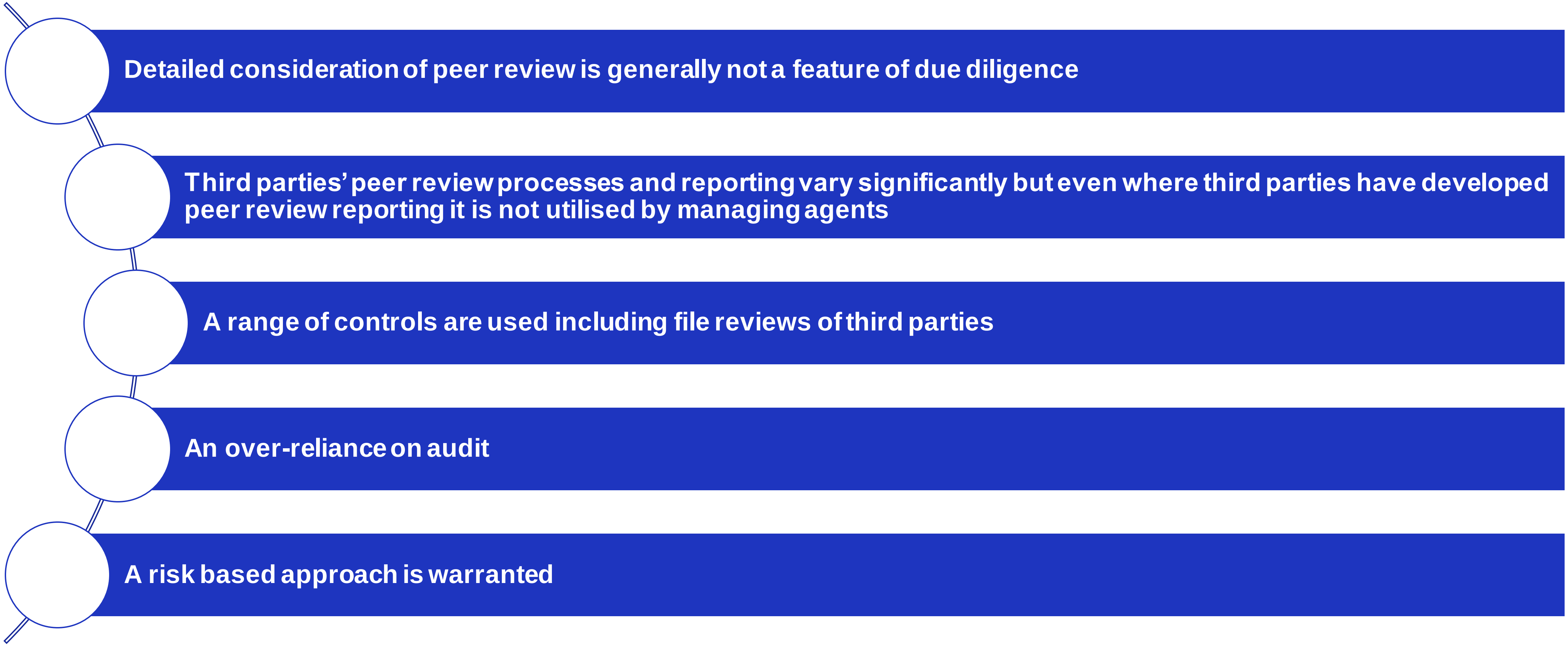
Effective use of peer review in overseeing delegated authority activity – why this subject?

- Findings from the Delegated Underwriting Claims Management 2017
- Use of peer review or file review as a control and qualitative assessment tool
- Oversight of the quality of decision making when delegating underwriting or claims authority
- Ensuring that customers are being treated fairly and communicated with appropriately
- Seven participating managing agents and discussions with six third parties
- Finding and guidance released to managing agents in February 2019

What we wanted to know

- How is quality of decisions overseen?
- Is peer review used as a control? If it is how?
- Are third parties asked to share their own peer review results? How do managing agents incorporate this into their own frameworks?
- Are third parties peer review processes assessed? How does this assessment influence the level of reliance placed on them?
- Do managing agents carry out their own file reviews? At what frequency?
- Where alternative controls are used, do these address the risks we are looking at? i.e. risk of poor decisions and risk of customers not being treated fairly

Key findings



Detailed consideration of peer review is generally not a feature of due diligence

Third parties' peer review processes and reporting vary significantly but even where third parties have developed peer review reporting it is not utilised by managing agents

A range of controls are used including file reviews of third parties

An over-reliance on audit

A risk based approach is warranted

Our expectations

- Understanding the risk & required controls
- Assess the adequacy
- Set expectations
- Monitor quality of decision making & customer outcomes
- Be clear on the purpose of audit and set clear & meaningful scopes
- Ensure alternative controls are reliable

What does this mean for you?

- Clearer instruction and scope – making you aware of the process expected to be in place
- An understanding of the level of reliance being placed on the control
- Is the peer review process working in line with what is understood and expected?
- Are there alternative controls that are expected to be in place?
- How effective are these process? Is the level of reliance right?
- Increased focus on the qualitative aspects when reviewing files rather than just the process – identifying any concerns that need to be addressed from on-going oversight and feeding into the scope
- Move towards review the reviewer

Audit scoping exercise and feedback – What does risk-based scoping look like?

Leena Ekman & Kate Czamara-Newton, Lloyd’s

Facilitated by MA’s, Auditors and Lloyd’s

Objective

The objective of the session is to improve the quality of audit scoping and ultimately reports produced and recommendations arising.

This exercise will attempt to find the top 5 -10 top risk factors to consider when scoping, these will then be incorporated into the Audit Scope Guidance document.

Minimum Standards MS9

CS 8.6 Audit programme

Managing Agents must ensure that Third Parties are subject to regular and appropriate audit. Managing Agents must establish and keep under review an audit programme which must be reviewed at least annually, having careful regard to Product Risk and Management Information relating to Third Party performance.

Managing Agents must:

- **set and record an appropriate scope for each audit, designed to assess compliance with contracted terms and quality of services being provided;**
- ensure that the person selected to undertake an audit of a Third Party has the necessary skills, competence and experience to do so;
- **provide the person selected to undertake an audit with all information necessary to conduct that audit;**
- **ensure the person who carries out the audit conducts an objective and evidence based assessment of the Third Party, with the output suitably recorded;**
- **promptly identify areas of non-compliance, shortfalls in capability or under performance;**
- communicate the results of the audit to the Third Party with any corrective action followed through to prompt resolution; and
- regularly consider the suitability and effectiveness of each audit firm being used

Code of Practice

Audit Scope

An appropriate audit scope will be determined by the Managing Agent for each Coverholder audit they arrange, which will be communicated to the auditor in advance of the audit as part of the terms of reference. Lloyd's strongly recommends that the LMA Risk Based Audit Scope be used as a basis for the audit, although individual circumstances may require a bespoke scope to be prepared. While it is not expected that Managing Agents will require the full scope to be used every time a Coverholder is audited, consideration should be given to the areas to be covered.

When scoping the audit, the Managing Agent should review the risk profile of the Coverholder and due diligence information held on the Coverholder; the audit should be used to test the Coverholder's processes and controls, not for information gathering. Managing Agents should consider those areas which have been tested previously or that represent a higher risk in order for the audit to address the requested areas in sufficient detail.

Workshop

We will be discussing 3 sections of the Risk Based Scope, each table having one to discuss.

The following sections of the scope have been chosen for this exercise:

- Underwriting
- Claims
- Customer Outcomes

You will have 45 minutes to discuss scoping and what factors would influence the scoping for your section.

We would ask you to list your top 5 factors to consider when scoping and to provide feedback on

- **3 things that work and**
- **3 things that could be improved**

We will then ask you to feedback your findings to the room and we will ultimately compile these and incorporate them into the Audit Scope Guidance document

Lunch and networking

LLOYD'S

Auditor Accreditation

Paul Brady, Head of Policyholder & Third Party Oversight, Lloyd’s

Mark Taylor, TurnStone Insurance and Reinsurance Services

Nick Barnaby, Manager, Lloyd’s

Auditor Accreditation

Paul Brady, Lloyd’s

At last year's conference we made the following proposals:

- To promote continuous education and knowledge of auditors;
- To ensure that auditors have the right skills given scope of audit;
- To provide a worldwide community of auditors;
- To give the market confidence in auditor selection; and
- To provide a public demonstration of your ability, skills and experience.

Which was met with broad support from those in attendance.

So this is what we've been doing since then:

- A working group was set up to develop the concept, with attendees from an audit firm, a managing agent, the LMA and Lloyd's meeting fortnightly.
- We have considered the criteria for accreditation and what ongoing training requirements should apply.
- The required enhancements to AiMS have been assessed and will be developed shortly.
- Engagement with DAG and DARA, both of which are supportive.
- Consultation with Auditors and LMA before finalisation of requirements by June 2019.
- Workshop with auditors tomorrow morning.

LLOYD'S

The Case for Accreditation

Mark Taylor, TurnStone Insurance and Reinsurance Services

Why is this needed?

- To improve the standard of auditors and create a reliable panel of auditors through AiMS.
- Managing agents can make a more informed choice of auditor based on the coverholder's risk profile and on the auditor's skills, expertise and experience.
- Managing agents all have their own panels, but the due diligence and TOBAs utilised vary considerably.
- Coordinated audit allocation can result in managing agents choosing between accepting the auditor supplied via AiMS or opting out. This can potentially lead to increased audit cost for the managing agent and push back from the coverholder at having to host a separate audit.
- The RFI information on AiMS is currently not detailed enough and needs enhancement. It only requires evidence of PI cover, CVs, and confirmation of completion of Lloyd's training modules.
- Auditors on AiMS need to be used by and 'proposed' / 'sponsored' by only one managing agent.

What does this mean for auditors?

- Formal recognition that they are an Auditor at Lloyd's, which will incentivise auditors to be (and remain) accredited.
- The accreditation will be useful for marketing to non-Lloyd's clients.
- It is accepted that there is a shortage of younger Lloyd's auditors; hopefully new auditors will be attracted into the Lloyd's space.
- Accreditation can be withdrawn for non-compliance and poor performance.
- There is a possibility that some auditors may not immediately reach the required minimum standard, so the roll out of the enhanced RFI will not be mandatory for 2019/20 but will be for 2020/21.

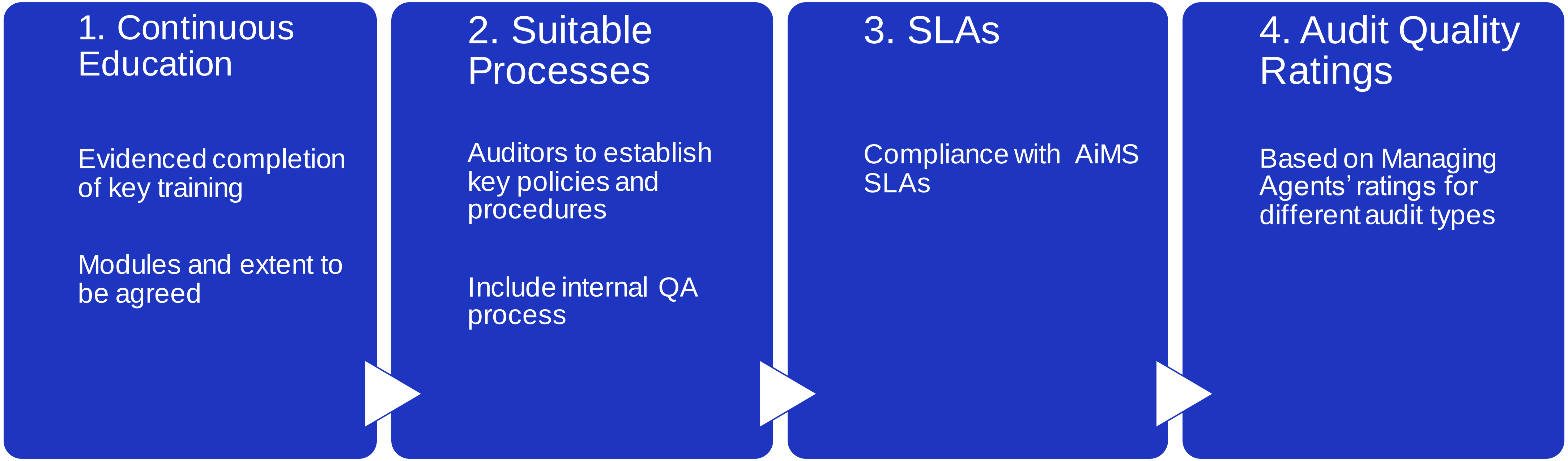
Market assistance

- The LMA are working on a new standard template TOBA between managing agents which is due out imminently.
- AiMS becomes a detailed database of approved auditors available to Manging Agents. The AiMS RFI and accreditation is intended to complement the managing agents' approach, not replace it.
- DARA is willing to support new and smaller firms to help with meeting the RFI standard.
- For non-DARA members, especially those outside the UK, I am happy to help and will feed any concerns you have back into the Working Group.

The Proposed Accreditation Process

Nick Barnaby, Lloyd’s

Proposed ‘4 Pillars’ for Accreditation



1. Continuous Education

Evidenced completion of key training

Modules and extent to be agreed

2. Suitable Processes

Auditors to establish key policies and procedures

Include internal QA process

3. SLAs

Compliance with AiMS SLAs

4. Audit Quality Ratings

Based on Managing Agents’ ratings for different audit types

What does this mean for managing agents?

- Greater information on existing auditor performance across the market gives comfort on service being provided;
- More granular information on competencies should assist in selection of auditors;
- Higher level of expectations around auditor internal processes (including QA processes) should lead to more consistent and improved output.
- Improved recognition of auditors should lead to increase in depth of audit resource;
- Assists in complying with Regulatory Expectations:
  - The FCA's DA Outsourcing Thematic Review TR15/7 made reference to "the amount and experience of the (audit) resource used" (3.123).
  - Lloyd's Customer Minimum Standards MS9 (CS8.6 Audit Programme) states that managing agents must *'ensure that the person selected to undertake an audit of a Third Party has the necessary skills, competence and experience to do so'*; and *'regularly consider the suitability and effectiveness of each audit firm being used'.*

TPA Audits

Scott Kellers, Head of Claims, Liberty

Lorraine Calway, GoldSeal Audit & Compliance

Claims Audit Scope

Scott Kellers, Head of Claims, Liberty

INSIGHT CONSENSUS INFLUENCE

Background

Lloyd’s Thematic Review – 7 Aug 17

- Over-reliance on audit as a control – greater focus required on other oversight methods
- Greater focus on technical file handling required and delivery against SLAs
- Greater co-ordination of audits required

INSIGHT CONSENSUS INFLUENCE

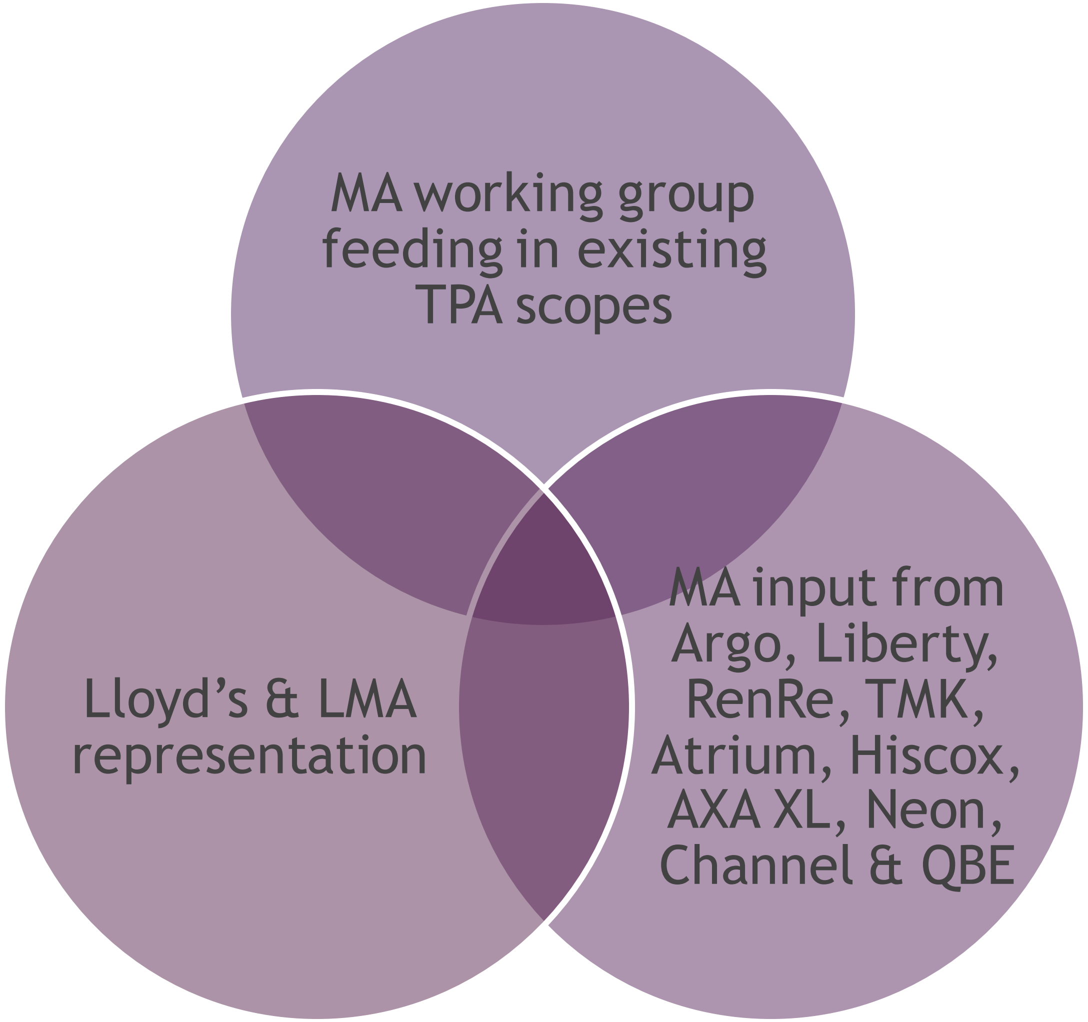
INSIGHT CONSENSUS INFLUENCE

Development - Background

Existing CH Audit Scope & Guidance

- In play since May 2017 (Pilot)
  - Risk
  - Control
  - Conclusions
- Positive adoption by MAs
- 670 CH Audits

Development – Market Input



MA working group feeding in existing TPA scopes

Lloyd’s & LMA representation

MA input from Argo, Liberty, RenRe, TMK, Atrium, Hiscox, AXA XL, Neon, Channel & QBE

CH Audit Scope / Guidance V2.0

Updates made to CH Audit Scope

- Additional Risks Added
  - Loss Fund Management
  - Bordereau Reporting
- Additional Guidance
  - Main focus on Claims Controls

INSIGHT CONSENSUS INFLUENCE

TPA Audit Scope / Guidance V2.0

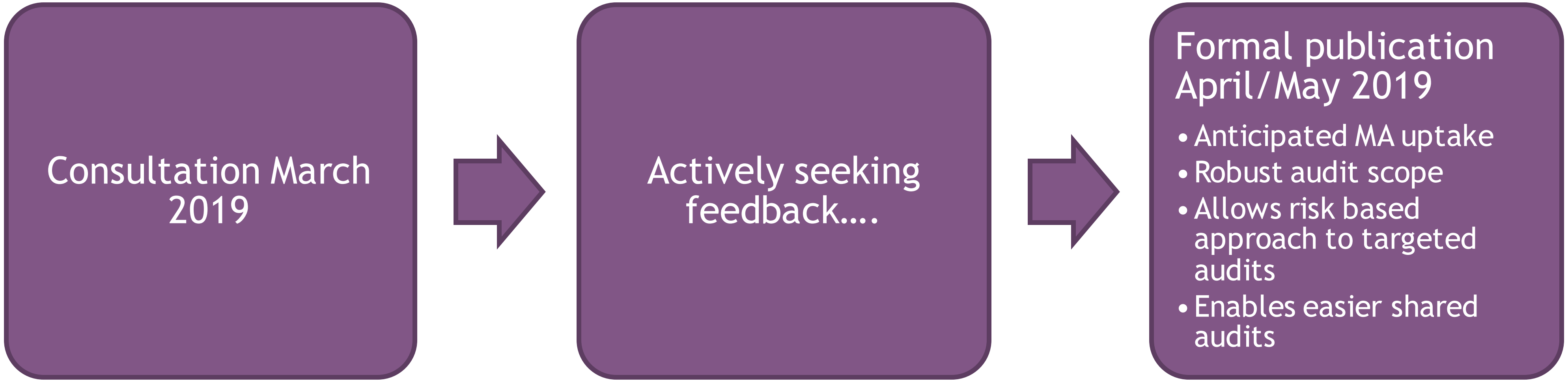
1. Underwriting
2. Underwriting Testing
3. Contract Documentation
4. Claims Controls With Authority
5. Claims Controls Without Authority
6. Claims Testing
7. Accounting
8. Accounting Testing
9. Reporting
10. Compliance
11. IT/Information Security
12. Customer Outcomes

INSIGHT CONSENSUS INFLUENCE

Claims Testing Template

- Review of audit areas and questions
- Focus to make robust claims examination
- Required to address lack of focus on claims decisions
- 38 questions > 61 questions
- Circulated 27/3/18 to all auditors
- Longer, but more thorough

Next Steps



Consultation March 2019

Actively seeking feedback….

Formal publication April/May 2019

- Anticipated MA uptake
- Robust audit scope
- Allows risk based approach to targeted audits
- Enables easier shared audits

INSIGHT CONSENSUS INFLUENCE

goldseal
audit and compliance

TPA Audit Scope

Lorraine Calway, Audit & Technical Services Manager, GoldSeal

CLAIMS TESTING

Does the file evidence that appropriate financial crime screening has been conducted prior to the release of claim payments and that outcomes were appropriately actioned and escalated?	***Review the payments to ensure that all payees have been screened against the required lists (eg. Sanctions, AML, PEPS).***

CLAIMS TESTING

Overall, did the claim deliver a fair customer outcome?	***Overall measure is whether the policyholder has been treated fairly, taking into account all the facts of the claim and whether the customer journey was reasonable in all the circumstances?***

goldseal
audit and compliance

CLAIMS CONTROLS

Due Diligence	***b) There is a discrepancy between the due diligence submitted annually and the actual position, resulting in unfounded assumptions of capabilities***

CUSTOMER OUTCOMES

Complaints Management	*d) Customers receive poor outcomes due to insufficient identification, investigation and resolution of complaints in accordance with regulatory requirements*

LLOYD'S

Cyber Security

Mo Philip, Senior Manager, Lloyd's

Nick Barnaby, Manager, Lloyd's

Agenda

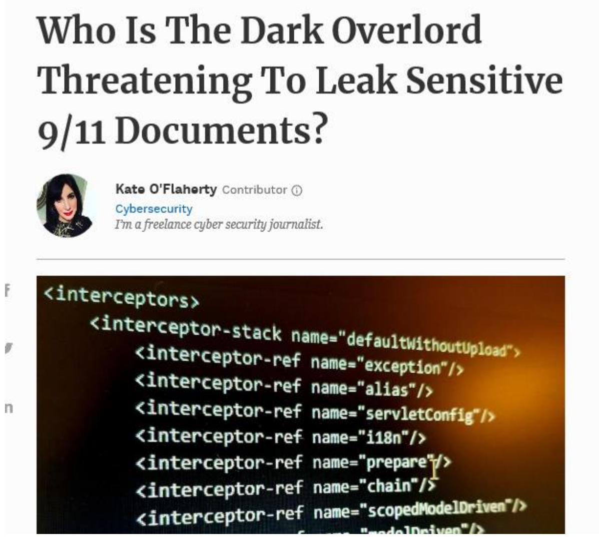
- Introduction – Cyber risk and Lloyd's
- What does good cyber hygiene look like?
- Questions

Introduction: Cyber risk and Lloyd's

- Lloyd's as an interconnected and global market
- A value chain with many links that can be exploited
- Lloyd's increasing reliance on technology and automation

- Our role as market leaders:
  - Thought leadership
  - Promoting cyber insurance

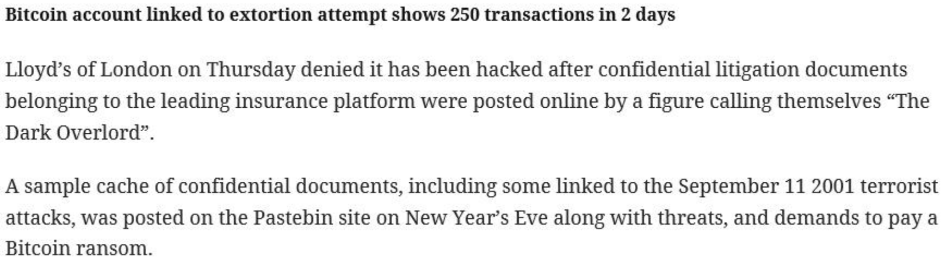
Introduction: Cyber risk and Lloyd's



Who Is The Dark Overlord Threatening To Leak Sensitive 9/11 Documents?

Kate O'Flaherty Contributor
Cybersecurity
I'm a freelance cyber security journalist.

```
<interceptors>
    <interceptor-stack name="defaultWithoutUpload">
        <interceptor-ref name="exception"/>
        <interceptor-ref name="alias"/>
        <interceptor-ref name="servletConfig"/>
        <interceptor-ref name="i18n"/>
        <interceptor-ref name="prepare"/>
        <interceptor-ref name="chain"/>
        <interceptor-ref name="scopedModelDriven"/>
```



Bitcoin account linked to extortion attempt shows 250 transactions in 2 days

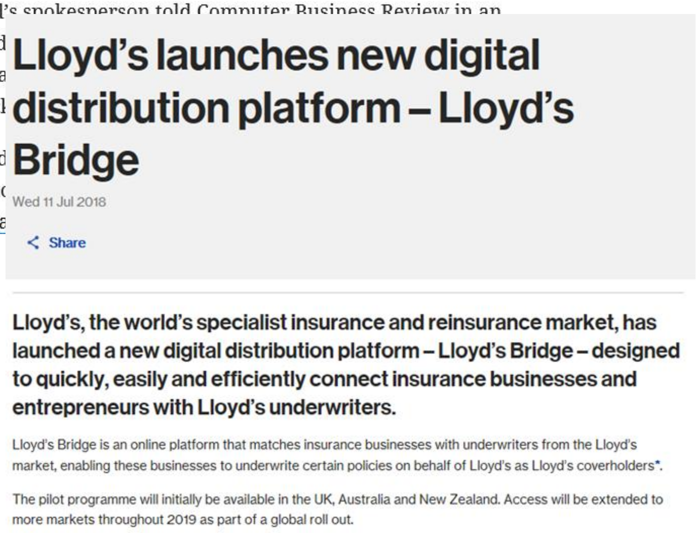
Lloyd's of London on Thursday denied it has been hacked after confidential litigation documents belonging to the leading insurance platform were posted online by a figure calling themselves "The Dark Overlord".

A sample cache of confidential documents, including some linked to the September 11 2001 terrorist attacks, was posted on the Pastebin site on New Year's Eve along with threats, and demands to pay a Bitcoin ransom.

Lloyds of London Hack Threats: "We Remain Vigilant"

A Lloyd's spokesperson told Computer Business Review in an emailed Corpora the hack

It is und were sto States la



Lloyd's launches new digital distribution platform – Lloyd's Bridge

Wed 11 Jul 2018

< Share

Lloyd's, the world's specialist insurance and reinsurance market, has launched a new digital distribution platform – Lloyd's Bridge – designed to quickly, easily and efficiently connect insurance businesses and entrepreneurs with Lloyd's underwriters.

Lloyd's Bridge is an online platform that matches insurance businesses with underwriters from the Lloyd's market, enabling these businesses to underwrite certain policies on behalf of Lloyd's as Lloyd's coverholders*.

The pilot programme will initially be available in the UK, Australia and New Zealand. Access will be extended to more markets throughout 2019 as part of a global roll out.

The global insurance industry, worth close to $1 trillion annually, has now become a prime target for cyber attack.

The sheer volume of valuable data created, gathered and stored by insurers presents a number of unique challenges for the sector. From a technical aspect, insurers are under continual pressure to modernize their data systems, facing the conundrum of keeping critical data highly secure yet also instantly available for review and processing.

> Not only do insurers possess this treasure trove of sensitive personal information, second only to government, but also increasingly rely on integrated information systems, providing multiple pathways for attack.
>
> - MWR InfoSecurity.com

Key definitions

- **Cyber risk** is the materialisation of the threat of attack, damage or unauthorised access to systems, data and / or services.

- **Cyber security** consists of technologies, processes and measures that are designed to protect systems, network and data from cyber crime. Effective cyber security reduces the risk of a cyber attack and protects organisations and individuals from the malicious or inadvertent exploitation of systems, networks and technologies.

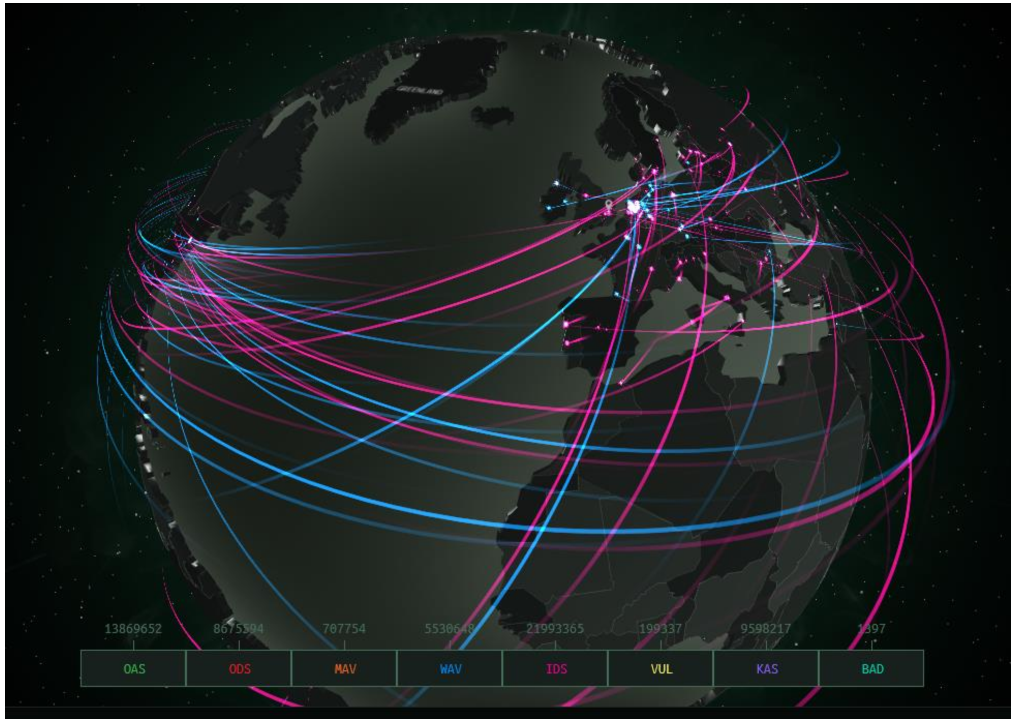
- **Cyber resilience** is a broader approach that encompasses cyber security and business continuity management and aims not only to defend against potential attack, but also to ensure your organisation's survival following an attack.

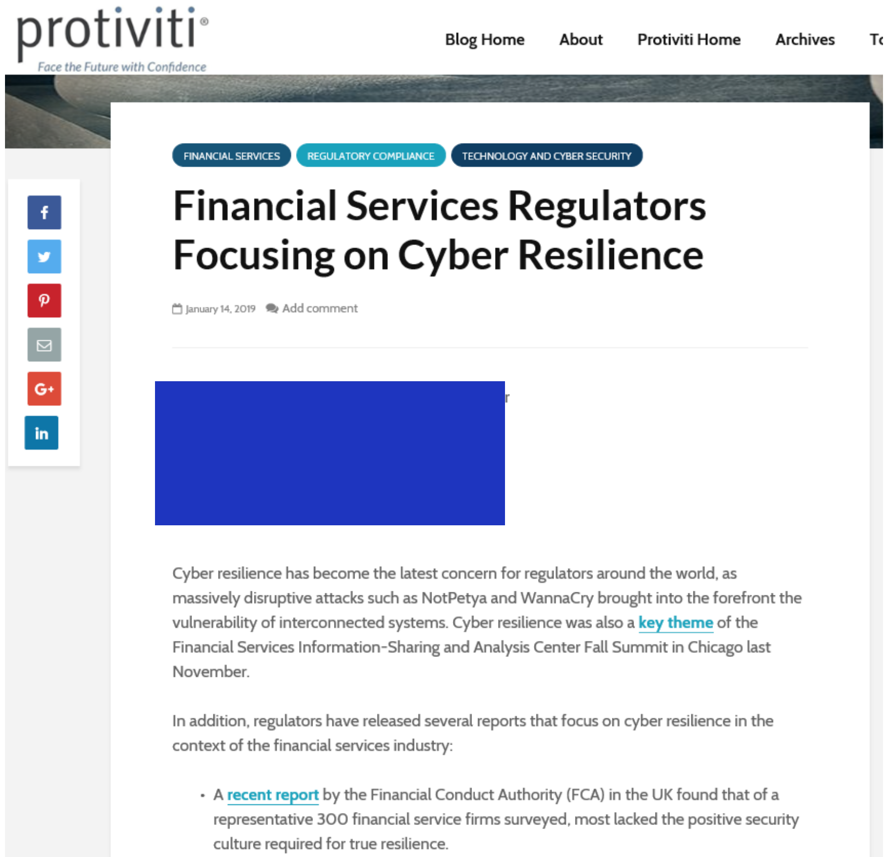
Cyber resilience = cyber security + business resilience

Cyber risk – the increasing threat

"Cyber resilience and cyber risk management are critical challenges for most organisations today. Leaders increasingly recognise that the profound reputational and existential nature of these risks mean that responsibility for managing them sits at the Board and top level executive teams"

World Economic Forum – Advancing Cyber Resilience Principles and Tools for Boards Jan 2017





Financial Services Regulators Focusing on Cyber Resilience

January 14, 2019 Add comment

[redacted]

Cyber resilience has become the latest concern for regulators around the world, as massively disruptive attacks such as NotPetya and WannaCry brought into the forefront the vulnerability of interconnected systems. Cyber resilience was also a key theme of the Financial Services Information-Sharing and Analysis Center Fall Summit in Chicago last November.

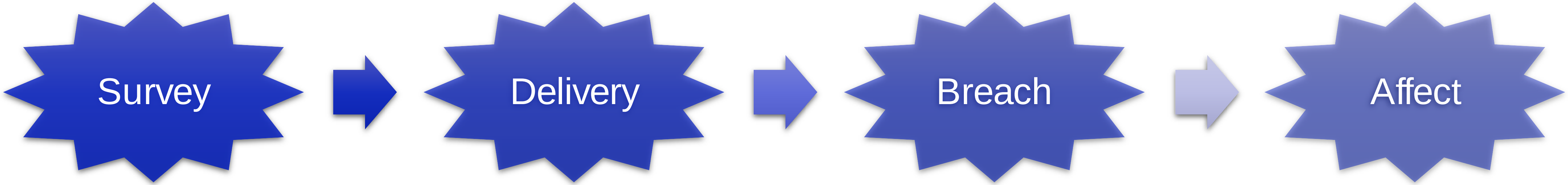
In addition, regulators have released several reports that focus on cyber resilience in the context of the financial services industry:

- A recent report by the Financial Conduct Authority (FCA) in the UK found that of a representative 300 financial service firms surveyed, most lacked the positive security culture required for true resilience.

Cyber risk – primary threat actors

- **Casual amateur** could be a teenager or a 'drive by' hacker; motivated by peer group kudos, the technical challenge or simply boredom.
- **Malicious insider** disgruntled or distressed employee; motivated by malice or financial reward, may have been placed or exploited by organised crime groups.
- **Trusted individual** typically an employee who makes an accidental mistake, leading to a cyber risk event.
- **Third party provider** a contractor or supplier who provides services to an organisation, they would typically have some level of access to systems and/or office premises. Cause of attack could be malicious or accidental.
- **Determined expert** either state sponsored groups, "hacktivist" groups or other individuals or groups motivated by financial gain, economic gain or geo-political reasons.

Cyber risk – key stages in an attack



Survey

Delivery

Breach

Affect

- **Survey** investigate and analyse available information about the target in order to identify potential vulnerabilities (technical, process or physical).

- **Delivery** getting to the point in a system that enables a vulnerability to be exploited, via email, infected USB, fake websites, compromise of legitimate sites.

- **Breach** exploiting a vulnerability/vulnerabilities to gain some form of unauthorised access. Examples: modifying system operations, gaining full control of a user's tablet, smartphone or computer.

- **Affect** carry out some activities within a system to enable to attacker to achieve their goals. Examples: stealing data, disrupting business operations, creating payments into bank accounts they control.

Cyber Attacks – Potential impact on Lloyd's and/or Coverholders

Successful cyber attacks could lead to:

- Fraudulent transactions
  - Hackers taking control of key bank accounts and diverting legitimate funds (e.g. claims payments) to wrong parties.
- Theft of sensitive personal data
  - Identity theft, fraud – enabling impersonation of key employees.
- Theft of sensitive company data, market data or other intellectual property
  - Enabling competitors to gain commercial advantage.
- Disruption to day to day business operations
  - Within individual service companies, managing agents or wider groups within the Lloyd's market.
- Damage to key parts of the information value chain
  - Undermining the integrity of data "how can we trust what's presented to us?"

Cyber Attacks – Potential impact on Lloyd’s and/or Coverholders

Impact of which could be:

- Regulatory sanctions relating to conduct or personal data theft (e.g. EU GDPR).
- Financial loss.
- Damage to the Lloyd’s brand, undermining the reputation of the market and its participants:
  - Customers taking their business elsewhere.
  - Managing agents / Coverholders exiting Lloyd’s market.
  - Less likelihood of new entrants to the market.
  - Market participants less likely to adopt new technology initiatives – less efficient market.
- Potential exposure to late payment penalties for claims.

Companies : Good Cyber Hygiene – Governance & Accountability

- Have a clearly defined cyber security strategy:
  - Set's out organisation's overarching strategy, aligned to business objectives
  - Includes an assessment of the current cyber risk landscape and the top cyber risks facing the business
  - Identify key assets/data sources critical to the organisation
  - Provide a roadmap of the current and future initiatives to enhance the existing cyber security framework
  - Must be reviewed on an annual basis to account for evolving threat
- Ensure that everyone in the organisation knows who is responsible and accountable for cyber at both executive and operational levels

Companies: Good Cyber Hygiene – Three lines of defence for Cyber Risk Management

Risk Ownership

(1st line : Operational Management)

- Identify, assess, manage and report digital risks on a regular basis
- Provide strategy for remediation activities and controls

Risk Oversight

(2nd line : Critical Partner)

- Provide independent challenge of material digital risk exposures
- Assess controls effectiveness for risk mitigation and against the risk framework
- Identify emerging risks, assess mitigating actions
- Support a risk based approach to market supervision
- Reporting to ExCo and Board Risk Committee

Risk Assurance

(3rd line : Independent Assurance)

- Provides assurance that the risk and control framework is effective
- Provide independent assurance on the internal control system, including testing design and operational effectiveness.
- Report to the Audit Committee and the Board

Companies : Good Cyber Hygiene - NIST Cyber Security Framework

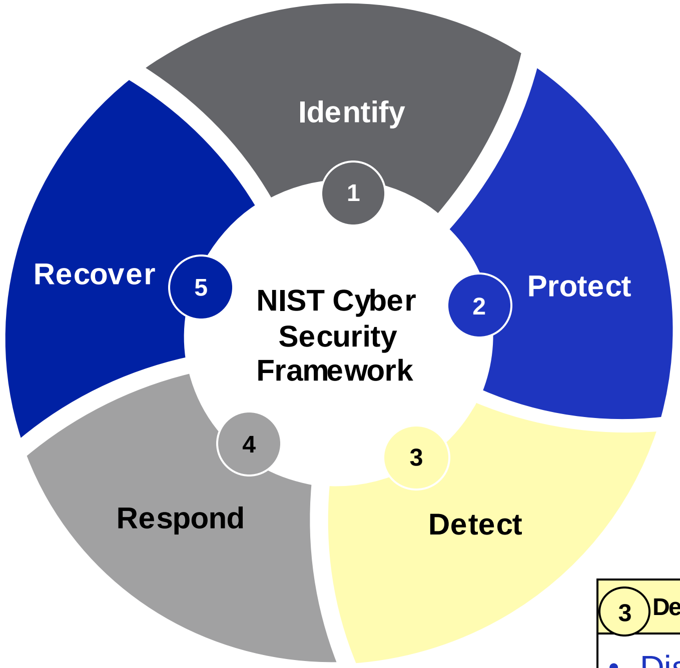
The NIST CSF provides a common language to understand, manage and express cyber risks both internally and externally. It can be used to help identify and prioritise actions for reducing cyber security risk and provides a tool for aligning policy, business and technological approaches to manage cyber risk.

5 Recover

- Maintain and test resilience plans
- Resume business operations

4 Respond

- Respond to Incidents
- Contain the impact of attacks



1 Identify

- Identify your 'crown jewels' or most critical assets
- Manage the risk in a proportionate way in line with Board defined appetites

2 Protect

- Safeguard systems and services
- Effective and comprehensive controls

3 Detect

- Discover malicious and or anomalous activities
- Alert relevant teams

Companies : Good Cyber Hygiene – NIST CSF (Identify)

- Develop a clear understanding of your most important ‘business services’
  - Those that are most important to you, your clients, counterparties, suppliers and customers
  - Ensure that third parties (e.g. loss adjustors, surveyors) adopt robust payment controls
  - Develop an automated method to validate the systems that are actually part of your IT network
- Understand the cyber risk, set risk appetites and associated tolerances:
  - Ensure that these are approved by and owned by the Board
  - Integrate cyber risk with your corporate risk management function

Companies : Good Cyber Hygiene – NIST CSF (Protect)

- Safeguard people, systems and services:
  - Ensure that all third parties (e.g. delegated claims authority) have received appropriate level of due diligence – in contracts and via assessments. For general cyber and for payment processes.
  - Deliver tailored training to 'high value' or 'high risk' employees e.g. those that are likely to be targeted or have access to privileged information.
- Implement effective and comprehensive controls:
  - Use multifactor authentication (e.g. something you know and something you have) for as many systems as possible, especially those based in the cloud.
  - Disable email auto forwarding rules whenever possible when using MS Office 365 and other cloud based email platforms.
  - Test the effectiveness of controls on a regular basis, either internally or via independent experts.

Companies : Good Cyber Hygiene – NIST CSF (Detect)

- Discover malicious activities:
  - Put in place monitoring on incoming and outgoing traffic
  - Develop an understanding of what ‘normal’ user activity looks like
  - Identify abnormal / anomalous activities and provide those alerts to the right team(s) in a timely manner
  - Consider bringing external specialists in to perform ‘threat hunting’ activities and penetration testing

Companies : Good Cyber Hygiene – NIST CSF (Respond & Recover)

- Respond to incidents in a timely and proportionate manner:
  - Appoint an incident manager supported by a virtual or actual team.
  - Make sure that everyone knows what their role is and who to contact in the event of an incident.
- Contain the impact of the incident:
  - Segregate the network and endpoints if possible.
  - Identify ‘root’ cause, conduct a comprehensive investigation.
- Maintain and test resilience plans:
  - Incorporate cyber specific scenarios in business continuity planning and testing.
- Resume business operations at the earliest opportunity:
  - Relies on everything mentioned above working well.

Cyber Security - Next steps

- Strengthening cyber risk oversight capabilities relating to Lloyd's market
- Improving collaboration between Lloyd's and Managing Agents
- Reviewing the adequacy of the current minimum standards

Coffee break

DAG Update

Tom Hamill, LMA

Peter Bolster, MS Amlin

Stuart Johnson, Axa XL

Delegated Audit Group Update

Tom Hamill, LMA

Peter Bolster, MS Amlin

Stuart Johnson, AXA XL

INSIGHT CONSENSUS INFLUENCE

Agenda

- Overview
- Reminder of purpose of DAG
- Issues discussed during the year
    - AiMS subgroup
    - Auditor TOBA
    - TPA Scope
    - Scenario Specific Coverholder Scopes
    - Large Coordinated Audit Survey
    - Other issues discussed during the year
- Key aims for the coming year

Overview
What is the Delegated Audit Group

Committee set up to help drive improvements to the audit process across the market, both operationally and in technical content.

Purpose:

To improve the quality and consistency of audits and to coordinate and drive improvements to the audit processes used by managing agents to monitor delegated underwriting and delegated claims arrangements.

INSIGHT CONSENSUS INFLUENCE

Membership of DAG

Chair: Peter Bolster, MS Amlin

Chris Morris, Brit

Andy Weeks, Argo

Gavin Smith, Hiscox

Nicola Major, AEGIS

Laura Pinto, Barbican

Ian Rankin, Amtrust

Paul Pampanella, QBE

Stuart Johnson, XL Catlin

Guy Sorce, Liberty

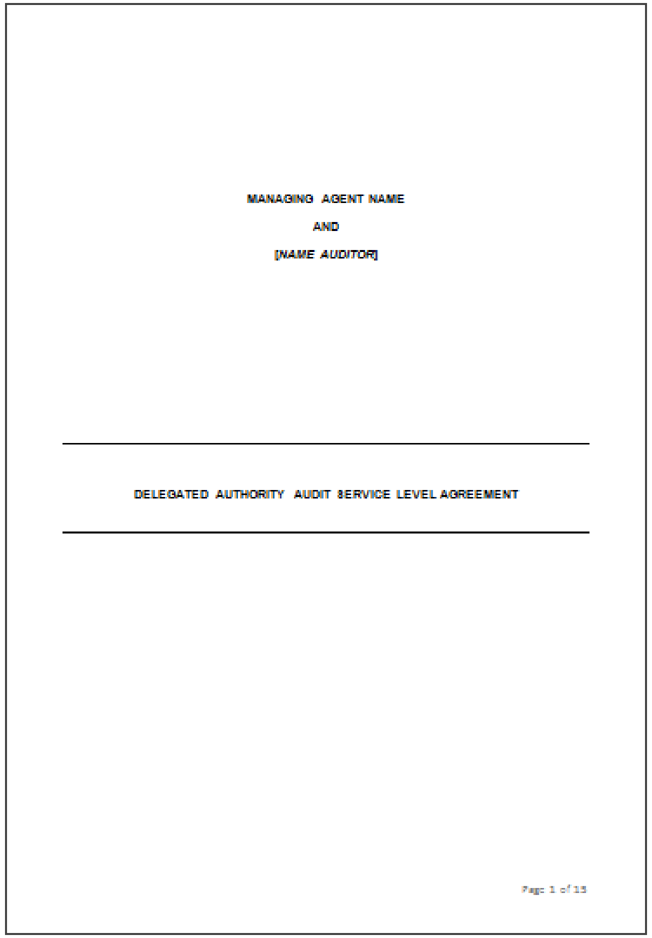
Leena Ekman, Lloyd’s

INSIGHT CONSENSUS INFLUENCE

INSIGHT CONSENSUS INFLUENCE

Auditor TOBA

- TOBA needed to assist with standardising terms and conditions.
- Will also assist with GDPR obligations.
- Legal review completed and content discussed with DARA.
- To be published shortly.



MANAGING AGENT NAME

AND

[NAME AUDITOR]

DELEGATED AUTHORITY AUDIT SERVICE LEVEL AGREEMENT

Page 1 of 15

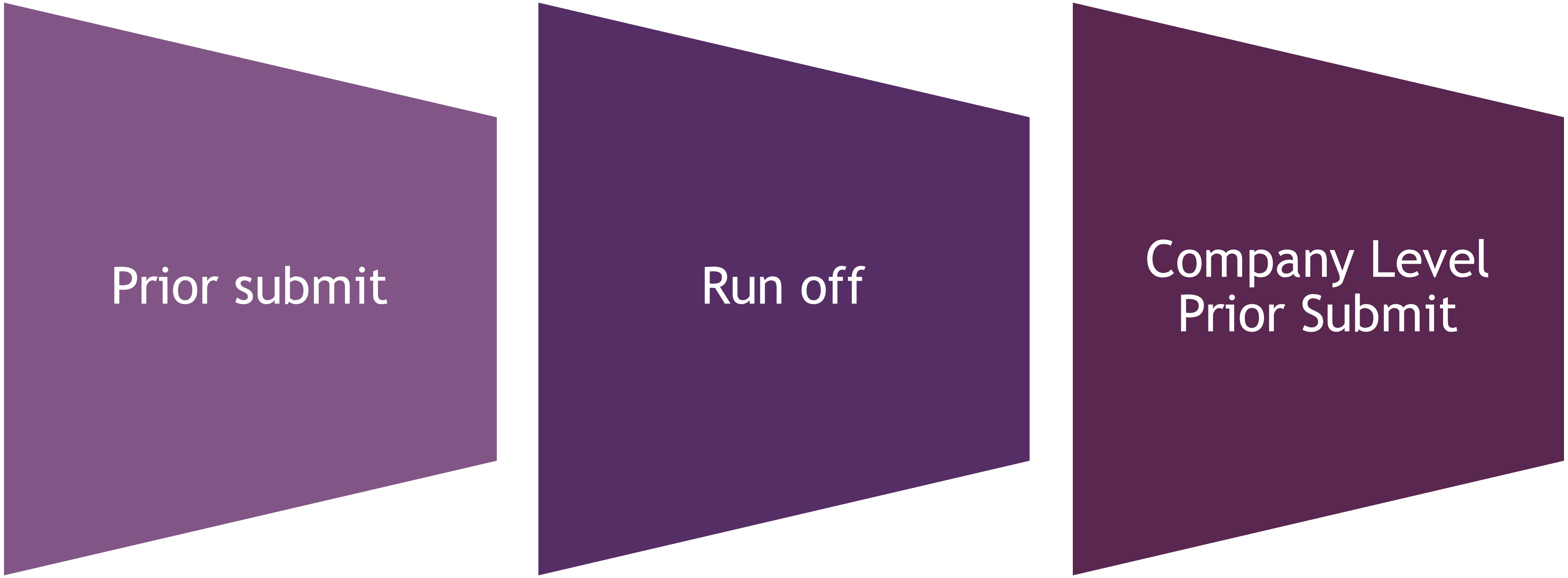
TPA Scope

- Work joined up with Claims Thematic working groups mid 2018.
- TPA scope and update to coverholder scope (for new claims section) out for consultation shortly.
- Same structures as coverholder scope:

  Risk – Control – Conclusion
- Increased focus on technical claims handling

Scenario Specific Coverholder Scopes

Specific sub sets of the existing scope designed to make scoping easier. Initially drafted by Turnstone as sub sets of the existing scope and now being considered by the DAG.



Prior submit

Run off

Company Level Prior Submit

INSIGHT CONSENSUS INFLUENCE

AiMS Subgroup

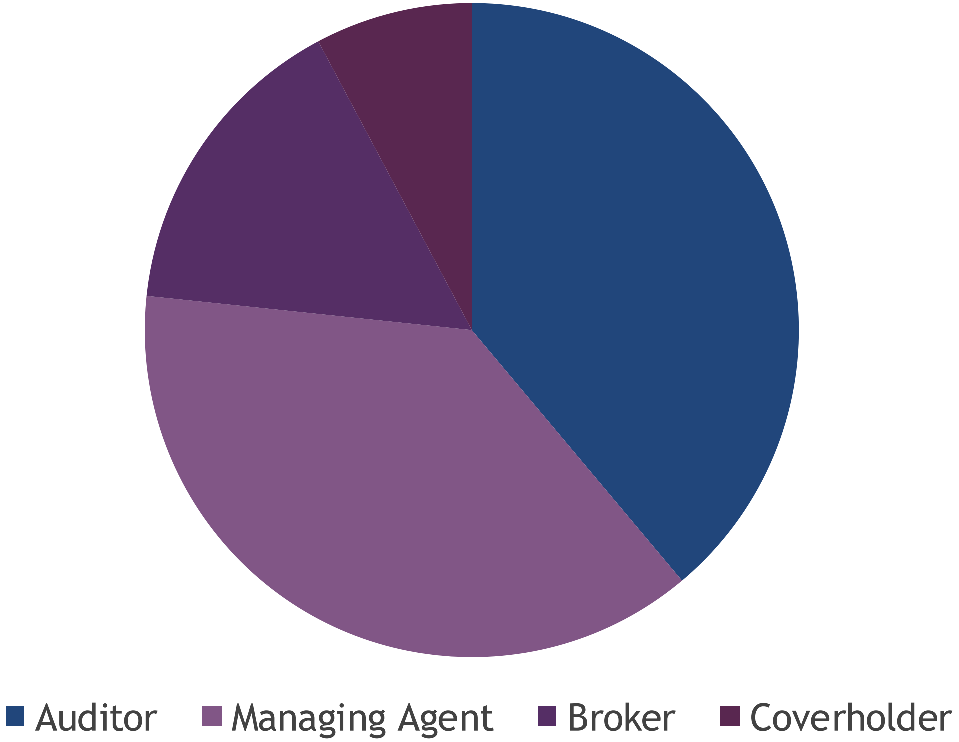
- Group assisting Lloyd’s with scoping and prioritising of additional requirements;
- Regular meetings with Lloyd’s;
- Now engaged with auditor and broker communities;

Large Coordinated Audit Survey

Purpose: To gather feedback from the market on what works on large coordinated audits and to draft best practice guidance for all stakeholders to improve standards

91

Respondents



INSIGHT CONSENSUS INFLUENCE

Large Coordinated Audit Survey Initial Findings - Definition

How do we define a large coordinated audit?

	Managing Agents	Auditors	Brokers / Coverholders
Participants	75% 3	91% 3	85% 2
Contracts	88% 1	100% 1	90% 1
Office Locations	75% 3	94% 2	63% 4
Classes of Business	78% 2	72% 4	72% 3

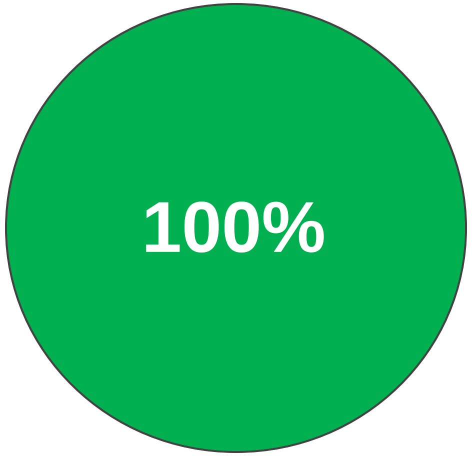
Percentages of ‘very important’ or ‘somewhat important’

INSIGHT CONSENSUS INFLUENCE

Large Coordinated Audit Survey Initial Findings - Key Contact

How often is a central coverholder contact point available to assist with coordination?

Brokers / Coverholders



Auditors

Always	32%
Usually	46%
Sometimes	11%
Rarely	11%

Only 1 auditor surveyed disagreed that having a central contact at the coverholder improved the audit experience

Large Coordinated Audit Survey Initial Findings - Peer Review

CHs	Do you have an internal peer review process?	93% Yes
MAs	Have you asked auditors to include peer review output as part of the audit?	65% No
	Would you consider doing so in future?	67% Yes
Auditors	Do you review output from peer review processes?	81% Yes
	Do you think there would be value in making greater use of peer review?	70% Yes

INSIGHT CONSENSUS INFLUENCE

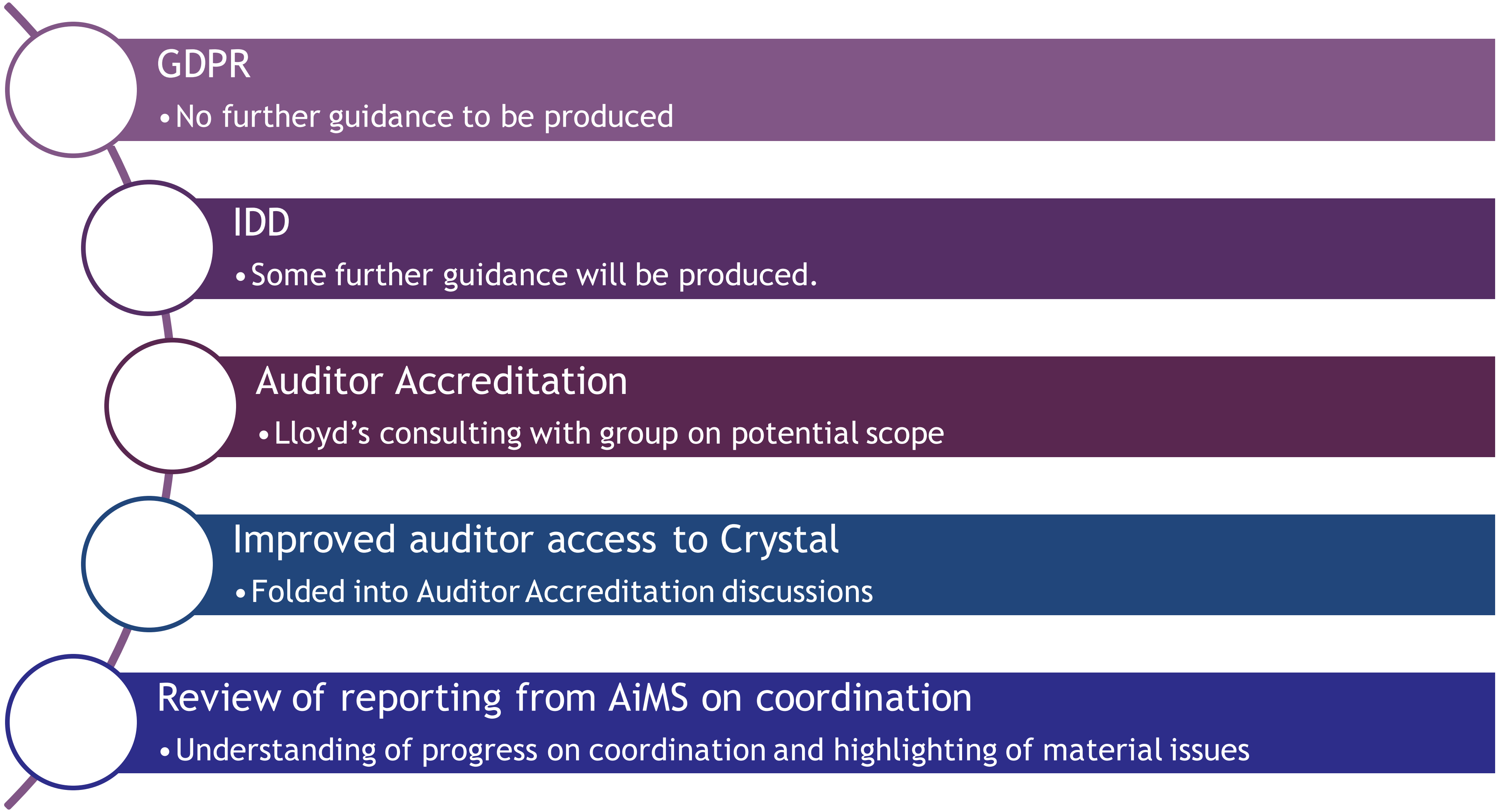
INSIGHT CONSENSUS INFLUENCE

Large Coordinated Audit Survey
Initial Findings - Remote File Review

CHs	Have you allowed auditors or MAs access to your systems remotely?	27% Yes
	If yes, did you feel this improved the audit experience?	46% Agree 9% Disagree
	Would you consider greater use of remote file review going forwards?	53% Yes
Auditors	Would you like to use remote file review more as part of audit?	36% Agree 21% Disagree
MAs	Have you asked auditors to use remote file review to undertake part of an audit?	78% Yes

Classification: Confidential

Other Issues discussed during the year



GDPR

- No further guidance to be produced

IDD

- Some further guidance will be produced.

Auditor Accreditation

- Lloyd’s consulting with group on potential scope

Improved auditor access to Crystal

- Folded into Auditor Accreditation discussions

Review of reporting from AiMS on coordination

- Understanding of progress on coordination and highlighting of material issues

Key aims for the coming year

- Continued work with Lloyd’s on AiMS enhancements
- Further work with Lloyd’s on Audit Coordination
- Data Security Scope
- Large Coordinated Audit Best Practice Guidance
- Assist Lloyd’s with Auditor Accreditation project
- Working closer with Auditor and Broker groups
- Further revisions to Coverholder / TPA Scopes if required

Suggestions for other issues for consideration on Slido please.

INSIGHT CONSENSUS INFLUENCE

Questions?

INSIGHT CONSENSUS INFLUENCE

Q&A Panel Session

Laura Pinto, Barbican

Paul Brady, Lloyd’s

Lorraine Calway, Goldseal

Leena Ekman, Lloyd’s

Tom Hamill, LMA

Jenny Neale, Lloyd’s

Ben Thomas, Lloyd’s

Mark Taylor, Turnstone

Wrap up

Paul Brady, Lloyd's

This information is not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to local law or regulation. It is the responsibility of any person publishing or communicating the contents of this document or communication, or any part thereof, to ensure compliance with all applicable legal and regulatory requirements.

The content of this presentation does not represent a prospectus or invitation in connection with any solicitation of capital. Nor does it constitute an offer to sell securities or insurance, a solicitation or an offer to buy securities or insurance, or a distribution of securities in the United States or to a U.S. person, or in any other jurisdiction where it is contrary to local law. Such persons should inform themselves about and observe any applicable legal requirement.

LLOYD’S