KPMG

Derbyshire Audit Forum

Venue – Derbyshire County Council

26 January 2017

John Cornett

Tony Crawley

Appendix 1

Agenda

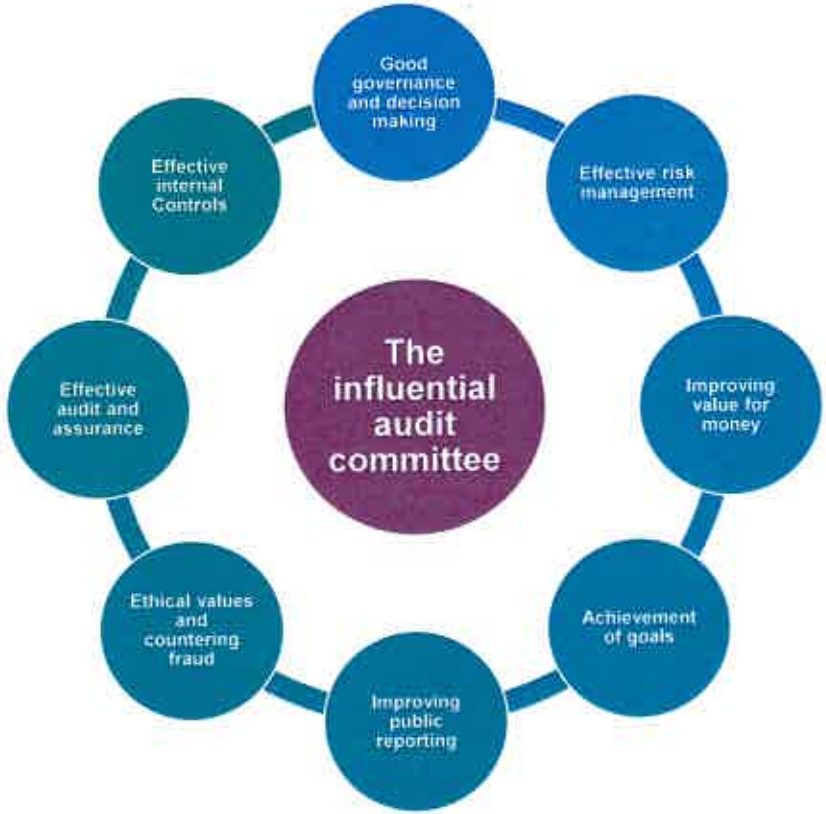
KPMG

Effective audit committees

Effective Audit Committees

'Audit Committees are a key component of corporate governance. They are a key source of assurance about the organisation's arrangements for managing risk, maintaining an effective control environment, and reporting on financial and non-financial performance.'

CIPFA



Audit Committees: Practice Guidance for Local Authorities and Police. *CIPFA December 2013*

Effective Audit Committees

What do you think makes an Audit Committee effective?

Effective Audit Committees

Characteristics of an effective Audit Committee

- **Membership –** Ensuring that the audit committee has the expertise and experience to provide robust oversight of financial reporting, audit quality, and other risks on the committee's agenda.

- **Active involvement –** In-depth knowledge of the organisation gained from (pro)active engagement and genuine interest in the organisation (beyond the boardroom).

- **Driving the audit committee's agenda –** The audit committee must shape its own agenda to ensure that it's risk-based, focused, and manageable.

- **Effective communication –** Open lines of communication with senior and middle management, internal and external auditors, and the full board based on mutual trust and constructive debate. "White space" time on the agenda for open dialogue.

Effective Audit Committees

Characteristics of an effective Audit Committee

- **Getting the right information –** Information provided to the audit committee must be relevant, concise, and timely.
- **Informal meetings –** Informal and ad-hoc meetings (in between regularly scheduled meetings) are essential to stay fully informed.
- **Tone at the top –** Sensitivity to the tone at the top of the organisation – and, indeed, throughout the organisation.
- **Leadership –** The attitude, skillset, and engagement of the audit committee chair are essential to achieving all of the above – which collectively drive the audit committee effectiveness.

Effective Audit Committees

Agenda management

- Is there a plan for the year to enable the Committee to meet its ToR?
- Who sets the agendas?
- Do reports map to the terms of reference?
- Do all Committee reports pass the 'so what' test?
- Do you assess whether you get the necessary assurance from each item?
- Is it clear who attends the Committee meetings and what you want from them?
- Do attendees know why they are there and the assurance you are looking for?

Effective Audit Committees

Meetings

- **Is there sufficient debate?**
- **Are decisions open?**
- **Do Committee members contribute evenly?**
- **Is the focus on quality of discussion rather than quantity of topics covered?**
- **Is there enough challenge and fresh thinking?**
- **Does the Committee take time to self-reflect, and ask for independent views?**
- **Do you recognise any of the issues in the ACI paper?**

Effective Audit Committees

The Committee's accountability for its role

- How do you provide assurance that you have delivered your ToR?
- Have Members' training needs been assessed and addressed?
- What impact has the Committee had?
- Have you assessed your effectiveness, and taken action where needed?
- Do you provide assurance that you have met your ToR – eg an Annual Report?

KPMG

Risk management (and the AGS)

Risk management - the basics

Simply……

The means to better identify and manage risks in a more co-ordinated manner in order to meet goals and objectives

Risk management is NOT…

…One event

…One size fits all

…Just about being compliant

…About eliminating risk

…The only answer to improving performance

Risk management IS:

…A series of actions

…About understanding your corporate objectives and how risks could affect their achievement

…A journey to improving performance and operational excellence

…Subject to the integrity of those accountable

…More than a process: "enterprise-wide" - culture, structure, policies, practice

…Owned by the Board – Practised by management

Risk management - the basics

An assurance structure includes each of the following three lines of defence:

Risk management - common issues

CONTENT	1	The risks contained in the risk register often don't reflect the real risks the organisation is running – identification/ measurement is wrong
	2	The risk assessment process by itself won't help manage risk better – you've got to understand the control environment and behavioural aspects
	3	Reporting of risk information is still largely compliance driven with observations focusing on the priority of risks rather than on control and improvement actions or developments of the risk management process itself
PROCESS	4	Selling the business case for risk management is still in the 'too hard' tray – many organisations don't have dialogue with their key stakeholders on risk management - investment and return are not clear, risk appetite is not known
	5	In many organisations executive management need to take more sponsorship and accountability for risk information and actively use it to improve performance and compliance
	6	Often there is no clear framework that co-ordinates risk management and internal control across the organisation – this can lead to confused management structures and policies surrounding risk and lack of focus for internal audit and assurance on what matters

Do you recognise any of these?

Risk management - choices

Risk appetite and control options

Your risk appetite is a key driver of your response to risks. But:

- **It depends on the level of risk**
- **It depends on your control options – which is partly driven by internal vs external considerations**

Risk management and the audit committee

The view from CIPFA

The role of the audit committee is to:

1) Seek assurance over governance risk
2) Keep up to date with the risk profile and the effectiveness of risk management;
3) Monitor the effectiveness of risk management arrangements and embedding good practice

Assurance over risk management is key to **THE** key element underpinning the Annual Governance Statement.

The audit committee should not manage or score the risks

Annual Governance Statement

What is it?

- **A review of the effectiveness of the council's system of internal control across all its activities.**
- **A Public report – promotes accountability.**
- **An open and honest self-assessment.**
- **An action plan to address significant and potentially significant risks.**

Annual Governance Statement

A good AGS should be ....

- **Open and honest**
- **A clear statement of actions**
- **Built upon a robust assurance framework**
- **Approved and owned at corporate level**
- **Reviewed and approved by Members separately from accounts**

Annual Governance Statement

What do you need to review the Annual Governance Statement (AGS)?

- **Knowledge of the governance framework of the organisation**
- **Understand the assurance framework that underlies the AGS**
- **Knowledge of the risks and internal control issues that have emerged during the year**
- **Be satisfied that the review of effectiveness is adequate**
- **Be satisfied that the action plans are realistic and meaningful**

KPMG

Cyber risk

Cyber risk - the key questions

High Level Question	Supplementary Questions
How secure are you currently?	What have been the most serious security and privacy incidents that you (and your peers) have faced in the past 12 months, what have you learned from those experiences, and what are you now doing differently to prevent them from re-occurring?
Are you getting more or less secure?	What key indicators are on your security dashboard, how is the organisation achieving those objectives, and how does this compare to your peers?
How do you set priorities and risk appetite ?	What is your organisational risk appetite for downtime, data loss and privacy incidents, how do you set your appetite level, and how are you tracking against that? What are the 'crown jewels' that require the highest levels of protection? Which business processes are critical to survival of the organisation?
How are you organised to manage the issue?	How is your first line and second line of defence set up? How do you report on the risk? How do you co-ordinate across multiple responsible functions?
Are you spending at the right level? And getting value for money for that spend?	What are you spending on security over the next three years? Is it enough to appropriately respond to the threat? Where are you under-invested and where can you make savings? Can you defend your investment compared to your peers?
How do you manage third party suppliers?	How do you ensure your suppliers (and their suppliers in turn) do not expose you to unacceptable cyber risk?


Cyber-Extortionists
Targeting the Financi
Sector Are Demand
Ransoms
LAW360
News, cases, companies, firms
'Cryptolocker' Virus Holdi
Data For Ransom
By Y. Peter Kang
ROBBED
BY CYBER
HACKER
Conmen who stole TalkTalk custo
details are raiding their bank accounts
Millions affected after cyber attack on HSBC
Caught, cyber bank
robbers who tried
Siphon off millio
JPMorganChase
STATEMENT
"Companies of our size
unfortunately experience
cyber attacks nearly
every day.
ASHLEY
MADISON®
Life is short. Have an affair.®
See Your Matches »
Morgan Stanley Acknowledges Insider Breach
By Jeff Goldman | Posted January 07, 2015
Morgan Stanley this week began notifying almost 10 percent of its

Ransomware attack

Email Received

- A member of Lincolnshire County Council opened a malicious email disguised as an invoice on the 26th Jan 2016.
- The email was opened and the malicious software was downloaded
- The type of attack is known as a 'zero day' attack. This is when the malware enters the system it can propagate itself easily as the antiviral software is unfamiliar with the software.

Data Encrypted

- Once on the system, all files on the council's server were encrypted becoming inaccessible to those wishing to use them.
- The types of data seized includes names, addresses, and medical conditions documented and dates of birth.
- The Council reported that there was no evidence that any of this information has been stolen.

Ransom Received

- The council received a ransom demand of £350 equivalent of the online currency, Bitcoin. The council refused to pay up.
- This was initially reported to be a much lager sum of £1 million.
- Once paid, the encrypted data would, in theory, be released.

Computer shutdown

The council was forced to suspend all use of their servers causing many services to be reverted back to pen and paper methods. Two days later, services were resumed as normal. No data appears to have been lost or stolen during the attack.

BBC Sign in News Sport Weather iPlayer TV Radio

NEWS

Home UK World Business Politics Tech Science Health Education Entertainment

England Regions Lincolnshire

Lincolnshire County Council hit by £1m malware demand

29 January 2016 Lincolnshire

Tech ark

Late

Ransomware shuts down UK council

Police investigate Lincolnshire County Council 'ransomware' attack

The Register

Biting the hand that feeds

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS

Security

Pay up, Lincolnshire, or your data gets it. Systems still down after ransomware hits

Council has shut down entire IT network to prevent spread

Cyber Essentials – Would it have saved Lincolnshire County Council?

Cyber Essentials – Foundations of Cyber Security

Lincolnshire County Council – hit by ransomware jan 2016

Around 28 January 2016, Lincolnshire County Council was hit with a ransomware attack. Initial reports from the BBC claimed the demands were for £1m. However by the end of the week the demand was reported as the more normal £300.

Ransomware can be devastating for home users. It has the potential to destroy priceless data. Few home users take proper backups and end up having to pay. This means there is a lot of money to be made.

Organisations are different. The assumption is they don't have backups. There is also an assumption they will never pay. This all means criminals very rarely target businesses with ransomware. What is likely to have happened is simply a user made a mistake and their email

This happens a lot. It is also one of the reasons why Cyber Essentials was created and why it is so valuable for businesses.

Would Cyber Essentials Have Helped?

Within the Cyber Essentials framework there are five security-centred areas. These are the foundations of good security.

Cyber extortion is a growing threat

Warwick Ashford

Security industry warns of increase attacks as Lincolnshire County Co ransomware demand

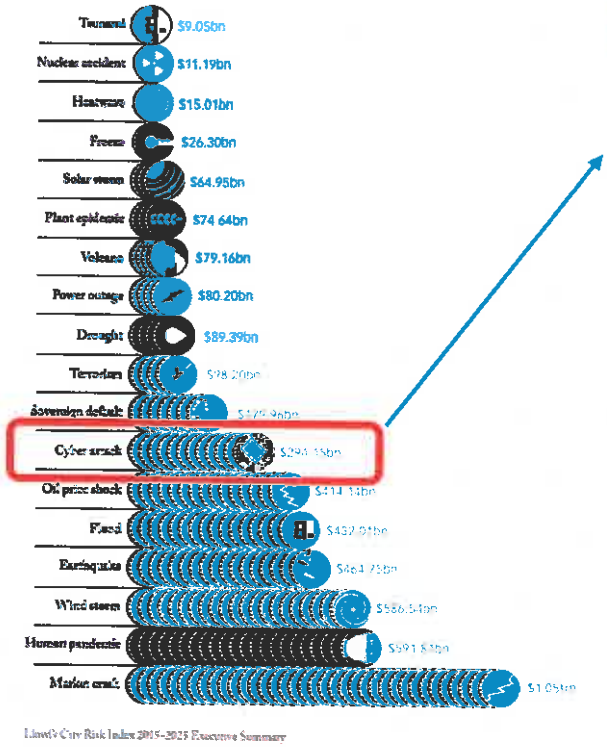
KPMG

What was the impact?

- The council suffered reputational damage;
- Library systems down (books were manually stamped);
- Online booking systems failed;
- Council main site halted;
- Financial losses;
- Productivity stifled.

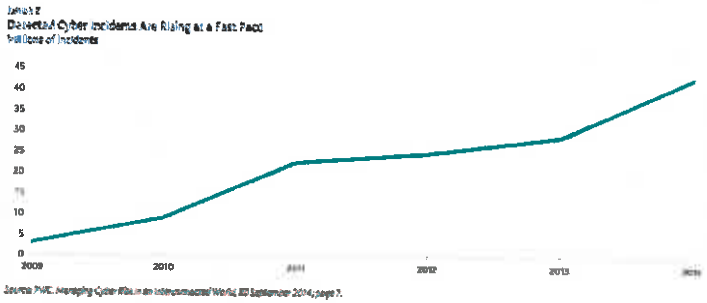
What did they do about it?

- Lincolnshire County Council acted as soon as the malware was detected preventing further damage
  - Therefore, only a small amount of their data was affected.
  - The Council had everything backed up so data affected could be restored.
- They worked with an outsourced security company to get their services back and running.
- The Council said it had notified the Information Commissioner's Office (ICO) about the incident, but said no personal data had been compromised.



Lloyd's City Risk Index 2015–2025 Executive Summary

RISK RANKING



Source PWC, Managing Cyber Risks in an Interconnected World, 30 September 2014, page 7.

Cyber Security Landscape

This is a "wicked" problem – multi-dimensional, unpredictable, intangible and constantly changing

Cyber Threats - It's a connected world

Who is being targeted?

WHO WOULD WANT TO TARGET US AND WHY?

THE INSIDER
Intentional or unintentional
Motivation: grudge, financial gain
Business impact: reputational damage, financial loss, regulatory censure

COMPETITORS
Competition or rivalry
Motivation: competitive advantage
Business Impact: competitive disadvantage

ISSUE MOTIVATED HACKERS OR 'HACKTIVISTS'
Attention or popular causes, may be / work with investigative journalists
Motivation: dynamic and unpredictable, potentially issue motivated
Business Impact: reputational damage, operational disruption

ORGANISED CRIME
Global, difficult to trace and prosecute
Motivation: financial advantage, potentially opportunistic
Business Impact: financial loss, reputational damage, operational disruption

STATE SPONSORED
Espionage and sabotage
Motivation: political and economic advantage
Business Impact: reputational damage, operational disruption, financial loss

INFORMATION

- CUSTOMER, SUPPLIER AND PERSONNEL DATA
- INTELLECTUAL PROPERTY
- COMMERCIALLY SENSITIVE INFO
- BUSINESS PROCESSES

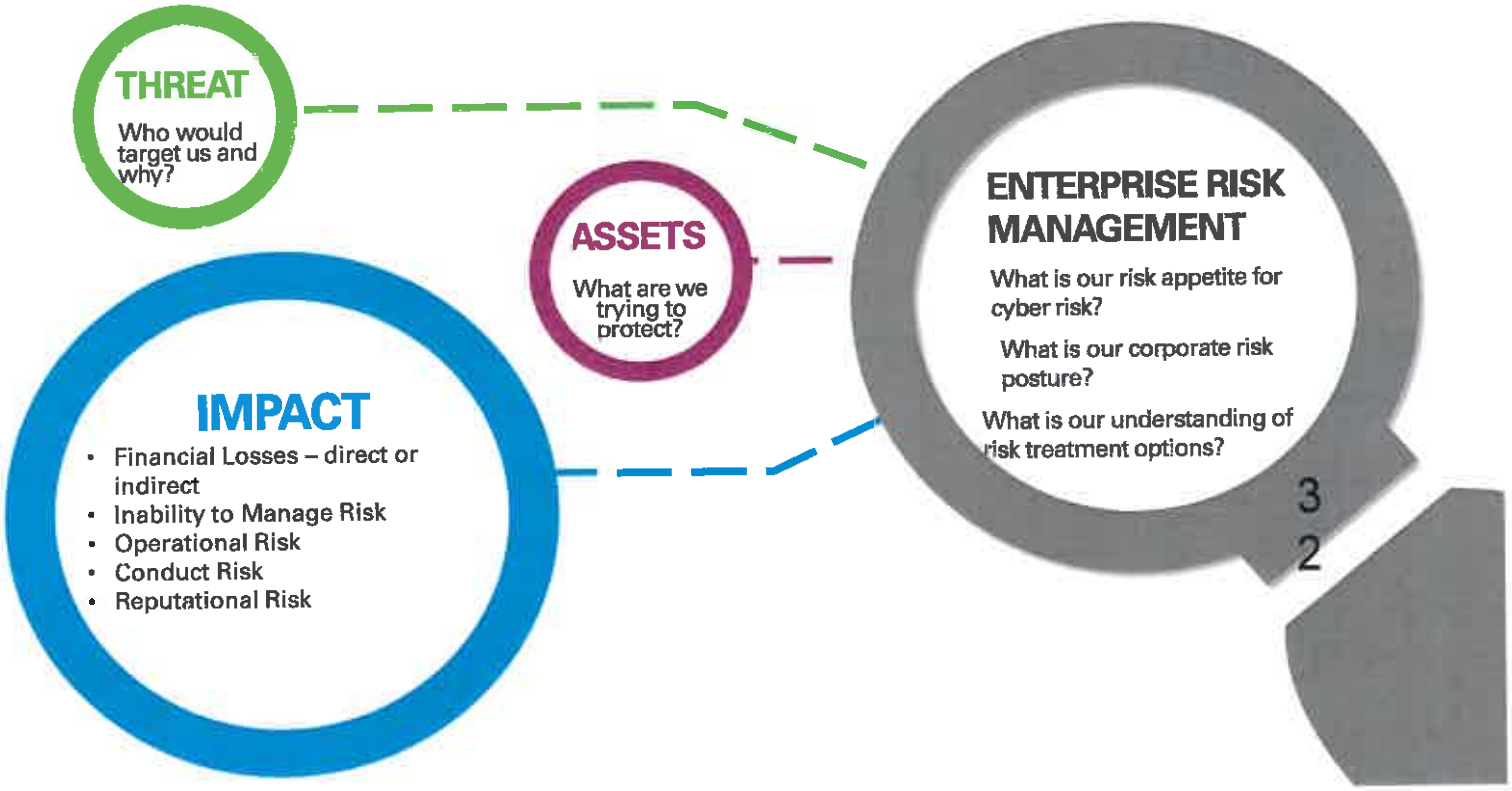
SERVICES

- CUSTOMER CHANNELS
- TREASURY / PAYMENTS FUNCTIONS
- INFRASTRUCTURE

TRANSACTIONS

- CUSTOMER INSTRUCTIONS
- B2B TRANSACTIONS E.G. INVOICING, SETTLEMENTS
- PAYMENT CARD DATA (INC. CVC)

WHAT IS BEING TARGETED?



Key Questions - Different levels

The Board

Are we a security resilient organisation?

Will future acquisitions Change our security posture

Do our long term business plans change our information security risk position?

What do our clients think about our approach to information security?

Is our information security strategy adequately mitigating the threats?

Are we taking a consistent and efficient aporoach to information security risk globally?

COO & CIO

Are we spending the right amount on information security?

Do we have effective governance and control in place for information security?

Do I have the right strategy?

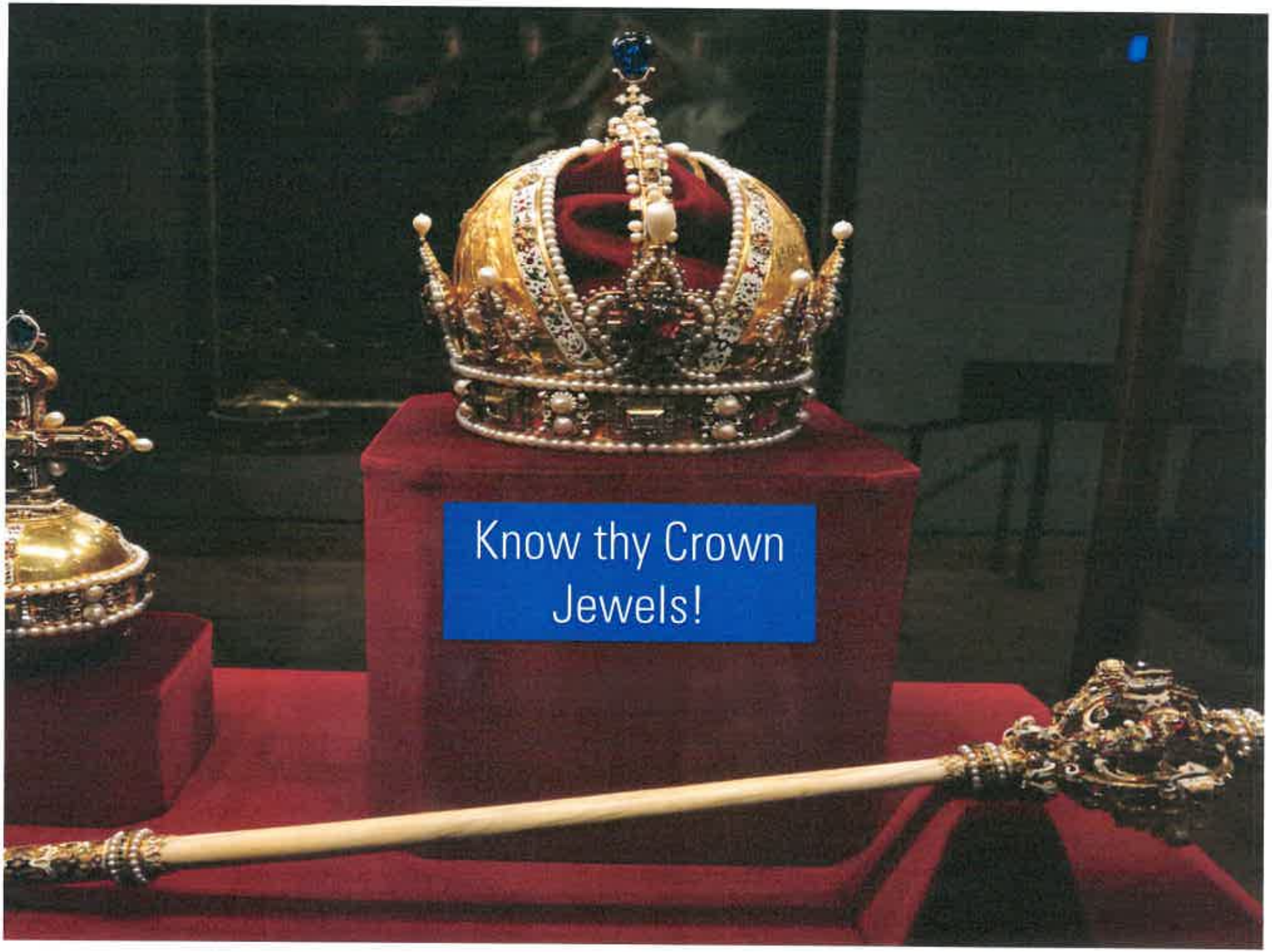
How does our security capability compare to our peers?

Head of Information Security

Am I investing in the right improvement projects?

Do I have the right talent and skills in my team?

Defending the Realm

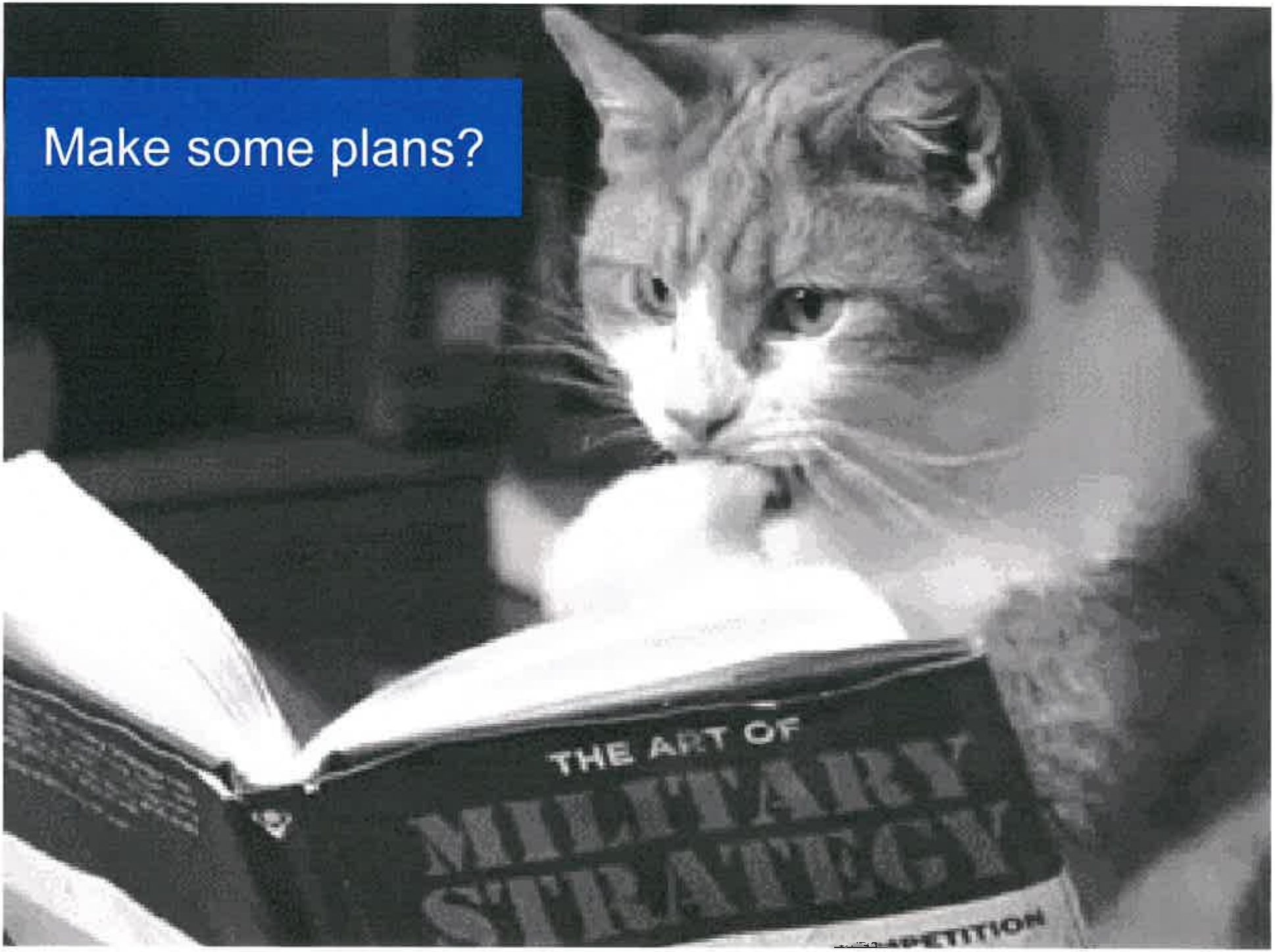

Know thy Crown
Jewels!


. . . but don't forget
dependencies


Where are your
crown jewels?

Could your crown jewels be.....

- **Shared with 3rd parties?**
- **In your supplier's networks?**
- **Scattered all around the place?**

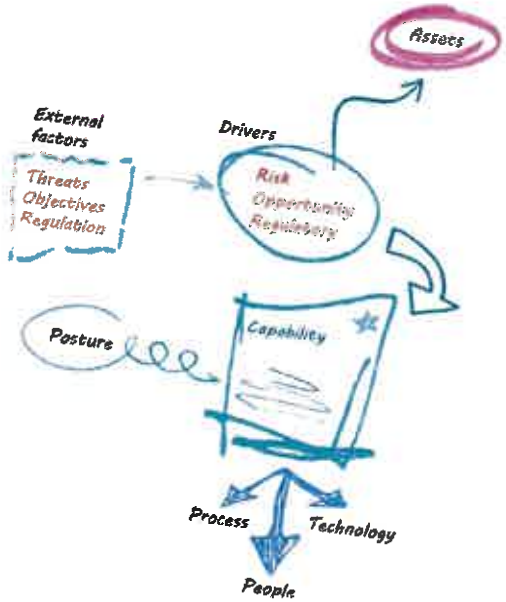

Make some plans?
THE ART OF
MILITARY
STRATEGY


Build some defences

Key things to have in modern cyber defence

- **Determination**
- **Data**
- **Knowledge base**
- **Team**
- **Money**

Response – How can these risks be mitigated



Common Mistake – The natural desire to find a technical solution to an inherently human problem leads to significant risks left unmitigated or inefficiently addressed

Getting the basics right - Cyber Essentials Scheme

Of the basic but successful cyber attacks against UK businesses and citizens of which Government has detailed knowledge, the large majority would have been mitigated by full implementation of the controls under the following, selected categories:

1. Boundary firewalls and internet gateways
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management

To implement these requirements, organisations will need to determine the technology in scope, review each of the five categories and apply each control specified. Where a particular control cannot be implemented for a sound business reason (e.g. is not practical or possible) alternative controls should be identified and implemented.

Source: Cyber Essentials Scheme Requirements

The Cost of Doing Business in the 21st Century

- Assume your organisation is a target.
- Assume your existing security controls can be bypassed.
- Apply the basics (patching, malware, education, leadership)
- Ensure you are able to detect and react to critical risk events quickly.
- Tap into external intelligence through providers and communities

Questions?

KPMG

Hot topics

Hot topics

As a starter . . .

EU General Data Protection Regulation (GDPR)

Hot topics - EU GDPR

Scale of fines for non-compliance - maximum fine capped at the greater of €20 million or up to 4% of total worldwide turnover.

Mandatory breach reporting within 72 hours

Requirement for Privacy Impact Assessments (PIAs)

No Safe Harbour

Required use of processors

Significant changes to consent requirements

Mandatory appointment of a Data Protection Officer (for some)

Right to erasure

Enhancement of Data Subject rights

Privacy by design

Increased security requirements

Inventory required

Requirement to register as a Data Controller likely to disappear

Mandatory Privacy policies

Increased transparency needed

Hot topics

What are your burning issues?

KPMG

Closing remarks

What next?

Are you interested in a Derbyshire Audit Forum?

If so…..

- **Would it benefit other members of your audit committee?**
- **What topics do you want to see covered?**
- **How often would you like to meet?**

But for now, thanks for coming today!

Thank you

Effective audit committee meetings: Warning signals and potential responses

Agenda overload is not a new issue for audit committees, but our latest ACI survey shows that it's becoming a major concern: 75 percent of the 1,500 audit committee members responding to our 2015 Global Audit Committee Survey said the amount of time required to carry out their audit committee responsibilities has increased moderately (51%) or significantly (24%) over the past two years.

So actual face-time across the audit committee table is really precious. Audit committee meetings should be well thought-out and structured in a way that allows the committee to make the most of its time together.

Effective planning and organisation can help ensure that meetings, are used effectively.

In brief, this could include:

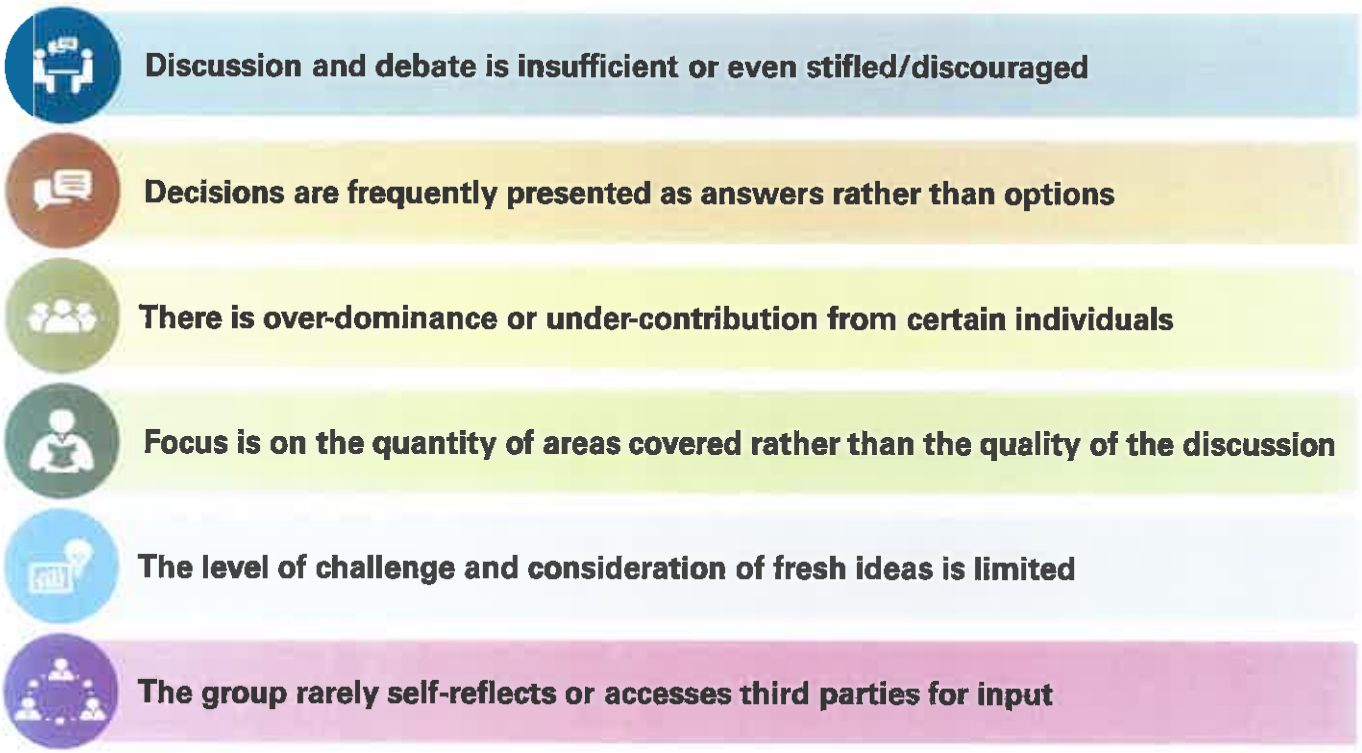
- Mapping out the calendar to ensure meetings cover all critical subject matter, but are still flexible enough for inclusion of urgent business when the need arises.
- Avoiding items that should be addressed in board or management meetings.
- Planning the specific agenda for each session ahead of time. Where possible the planned conversation should also be effectively framed so that the committee members know the purpose of each item. e.g. whether an item is for challenge, debate or "for information".
- Ensuring that committee members have access to the right information and papers in advance of the meeting.
- Identifying clear outcomes i.e. whether a decision or agreed position, and appropriate follow-up.

Inevitably there will be times where, despite a robust planning process, well thought out agenda and timely papers, meetings are still not as effective as they might be. The table overleaf identifies potential issues, the likely warning signals and offers some suggestion as to how the issues might be addressed.

Effective audit committee meetings: Warning signals and potential responses

		Potential responses		
Underlying issue	**Warning signals**	**Audit committee chair**	**Audit committee members**	**Management**
Overly dominant personalities or groups in the audit committee meetings controlling the debate	▪ Dissenting voices marginalised ▪ Difficult issues not sufficiently discussed ▪ Debate becomes personalised not issue focused ▪ Special insights not used ▪ Individuals appear reticent to speak up ▪ Third parties stereotyped as out of touch ▪ Management team is defensive or aggressive	▪ Build trust and respect with all members. Speaking with them ahead of meetings and make sure they are sufficiently briefed to contribute effectively ▪ Give weight to the views raised ▪ Lead by example showing that uncertainty and questioning of assumptions is appropriate ▪ Play 'devil's advocate' by offering a counter-argument to provide balance ▪ Encourage and give air time to new committee members, by asking for opinions ▪ Address directly with the chairman of the board if dominance continues	▪ Speak up but avoid dominating airtime ▪ Ensure you are fully briefed to offer alternative insights ▪ Add value by adding fresh insight ▪ Build relationships with other members and rehearse difficult questions or concerns before the audit committee meeting	▪ Seek to understand the knowledge levels amongst the committee members and address when members may be out of their depth and reluctant to contribute. ▪ Encourage calling out from induction onwards ▪ Consciously ask for input and advice ▪ Seek input from specific directors outside board meeting – does overall consensus reached reflect majority of individual opinions?
The audit committee is being 'managed' by the executive team in attendance	▪ Executive present answers rather than options ▪ Insufficient focus on the big picture/too much focus on operational matters ▪ Probing challenge not welcomed by the executive team ▪ Insufficient emphasis on risk ▪ Papers not tailored to board needs	▪ Use the company secretary actively in preparation of papers ▪ Pre-agree with relevant executives how particular issues should come to the committee ▪ Personally demonstrate behaviour required by querying judgements and assumptions ▪ Insist on meeting relevant executives ahead of papers coming to committee	▪ Respect the executive need for a instant decisions, but push back in the discussion ▪ Get to know the business and the people below the top executive team ▪ Be active conduits to the external world	Where management team is enlightened and keen to redress the balance ▪ Use scenarios to show the range of options being considered ▪ Use 'reverse stress testing' to demonstrate risk awareness and control ▪ Show willingness to suspend own assumptions and seek feedback on approach
'Groupthink' - The audit committee lacks diversity of thought	▪ Constant drive to get through the agenda and move on to next topic ▪ Scenarios rarely used ▪ Lack of any external input or challenge ▪ Assumptions not tabled openly ▪ Different options or ideas not presented or evaluated ▪ 'Out of the box' thinking discouraged	▪ Use a facilitative style to manage the debate ▪ Use third party briefings or facilitation to increase insight and facilitate opposing views ▪ Review the committee membership or their working styles to identify potential gaps in thinking – openly discuss this as a risk ▪ Review the style and effectiveness of the boardroom conversation	▪ Use 'intelligent naivety' to ask the 'non-obvious questions' ▪ Keep asking questions in different ways until satisfied ▪ Suspend prevailing assumptions ▪ Change the angle of debate	▪ Present options and alternatives rather than a fait accompli ▪ Actively request debate when positioning difficult issues seen as hanging in the balance ▪ Overtly welcome the committee's views ▪ Ensure the committee has all the relevant information to take a balanced view
The audit committee is overly focussed on process	▪ Overemphasis on ticking the boxes at the expense of open discussion or debate ▪ Inappropriate allocation of time to critical issues ▪ Sense of pressure to get through the agenda ▪ Failure to stand back and look at the big picture ▪ Unwillingness to challenge the way things are done	▪ Involve multiple inputs when setting the agenda ▪ Differentiate agenda items by importance ▪ Listen hard for signals of discomfort ▪ Don't be afraid to park items for further review where necessary ▪ Be prepared to call additional meetings where necessary	▪ Raise concern either in meeting or offline with the audit committee chair ▪ Offer to lead the discussion on a specific upcoming issue ▪ Specifically cover during the annual evaluation process	▪ Ensure committee members are properly briefed on critical issues and audit committee priorities ▪ Provide meaningful and constructive feedback if asked to contribute to the evaluation process ▪ Proactively volunteer constructive thoughts from outside the committee
Low commitment, engagement or capability of some audit committee members	▪ Attendance in person but not in spirit ▪ Lack of preparation is evident ▪ Consistent lack of contribution ▪ Focus narrowly on own perspective ▪ Too much shooting from the hip	▪ Get to know each member by spending time with them outside formal committee meetings ▪ Be clear and realistic with members about the contribution and commitment required from outset ▪ Encourage that mobile phones are switched off ▪ Change the committee's constitution if appropriate	▪ Raise any issues promptly with the audit committee chair ▪ Consider whether this is the right NED appointment for you and whether another position may provide greater engagement and job satisfaction	▪ Be sensitive to committee members feeling out of their depth or marginalised ▪ Discuss offline and encourage greater contribution, even in areas outside their domain specialisation ▪ Share own thinking process with committee members ▪ Set expectations of level of commitment and engagement early on at induction stage
Lack of reflection time about the committee's own performance, style and way of operating	▪ Little discussion on how debate could be improved ▪ No opportunities to consider 'what might be done differently or better next time' ▪ Process suggestions are put down ▪ Annual committee evaluation does not get to the real core issues	▪ Encourage occasional wide ranging discussion on meeting evaluation at post meeting dinners ▪ Meet with each director to gather their views on the quality of conversation/debate and get their suggestions for improvement ▪ Consider use of other tools to provide additional awareness e.g. team or personality profiling/evaluation or external facilitation	▪ Insist on the maintenance of high standards ▪ Use external experience to support behavioural change	▪ Provide meaningful and constructive feedback if asked to contribute to the evaluation process ▪ Proactively volunteer constructive thoughts from outside the committee

Warning signals to look out for during your audit committee meetings:



Based on Tomorrow's Company's Good Governance Forum's publication 'Improving the Quality of Boardroom Conversations'.

Contact

Timothy Copnell
Chairman, UK Audit Committee Institute

Tel: 020 7694 8082
Email: tim.copnell@kpmg.co.uk

Further reading and resources:

The ACI Audit committee handbook is packed full of useful tools:

Downloadhandbook