



Derbyshire Audit Forum

Venue – Derbyshire County Council
26 January, 2017

John Cornett
Tony Crawley

Agenda

14:00 Welcome and Introductions	14:00 – 14:30 What makes an effective Audit Committee?	14:30 – 15:00 Risk management – the basics	15:00 – 15:20 Break
15:20 – 16:00 Cyber security	16:00 – 16:40 Hot Topics	16:40 – 17:00 Closing remarks Future events?	17:00 Close

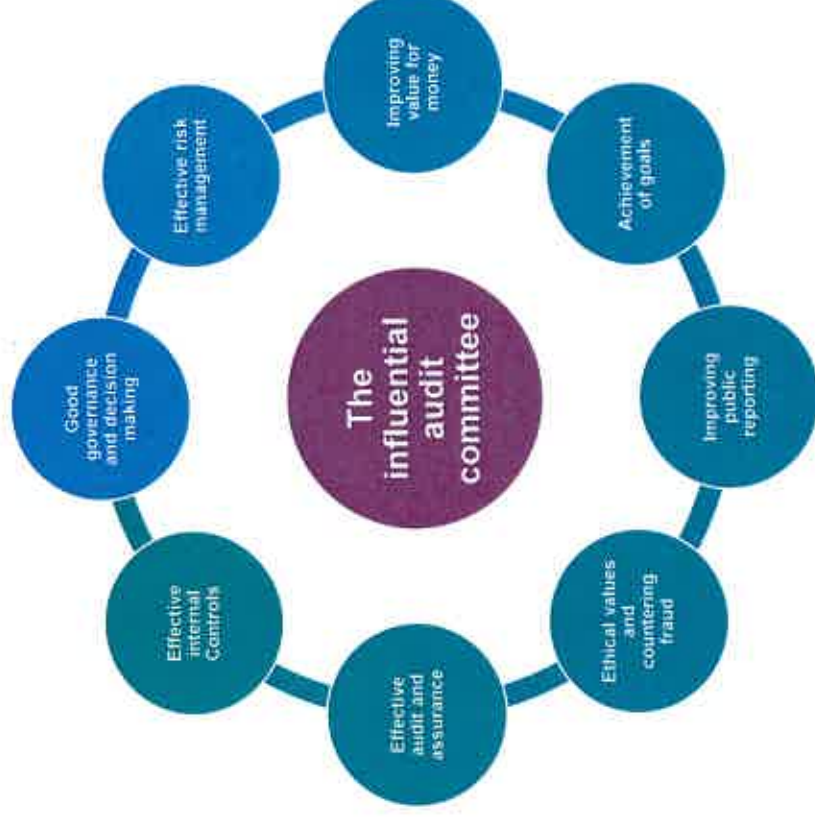


Effective audit committees

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

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?**



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 - 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
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
PROCESS	

Do you recognise any of these?



Risk management - choices

Risk appetite and control options

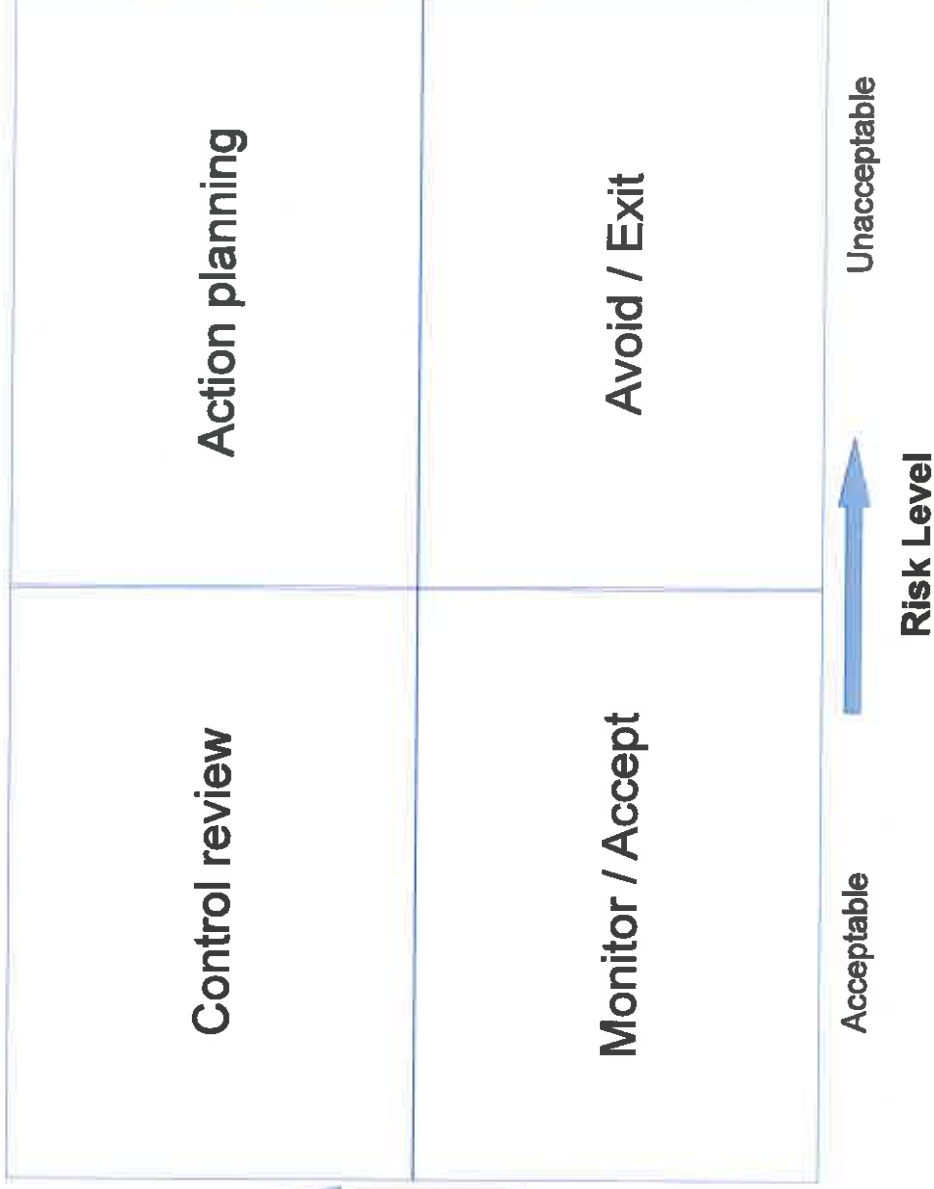
Your risk appetite is a key driver of your response to risks. But:

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

A lot more we can do

Control Options

Nothing more we can do



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

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**





Cyber risk

Cyber-Extortionists Targeting the Financial Sector Are Demanding

RANSOMS

News cases, companies firms

'Cryptolocker' Virus Holds Data For Ransom

By Y. Peter Hong

ROBBED BY CYBER HACKER

Common who stole TalkTalk customer details are raiding their bank accounts

Millions affected after cyber attack on HSBC
HSBC's website across the world have been hit by one of the largest
cyber attacks in the world that left millions of customers

Caught, cyber bank robbers who tried siphon off millions



STATEMENT
"Companies of our size
unfortunately experience
cyber attacks nearly
every day."

ASHLEY MADISON

Life is short. Have an affair.

Get started by going to your relationship advisor

Please Select

Use Your Mailings

Morgan Stanley Acknowledges Insider Breach

One of its 4.6 million Wealth Management

A former financial adviser allegedly stole 10 percent of the company's 4.6 million Wealth Management customers' account information.

By Jeff Gukovits | Posted January 07, 2015

Morgan Stanley this week began notifying almost 10 percent of its Wealth Management clients that an employee had stolen their



NEWS



the guardian



Ransomware attack



© 2019 KPMG LLP, a US limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG Network, a global organization of member firms affiliated with KPMG Network, a global organization of member firms.



England Regions **Lincolnshire**
Lincolnshire County Council hit by £1m malware demand

© 29 January 2016 Lincolnshire



Tech **Link** **Late**

Ransomware shuts down UK council



Police investigate Lincolnshire County Council 'ransomware' attack



The A Register
 Making the World Start Fresh

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 is a UK Government driven programme designed to help businesses of all sizes reduce the impact of ransomware attacks. It is a mandatory requirement for those who wish to be eligible for the award. The programme provides services to any other government departments including local government and schools.



This is a good thing. Ransomware has been a major issue for many organisations and it is good to see the government taking steps to help them protect themselves.

Justly not every government department has taken steps to protect itself. Around 20 January 2016, Lincolnshire County Council was hit with a ransomware attack. Local reports from the BBC during the attack were for £1m. Ransomware is a type of malware that encrypts files on the end of the work. The ransomware demands a payment of £100,000.

Ransomware can be devastating for some users. It has the potential to destroy personal data. Some users may take a longer time to get up and running again. This means some may have a loss of revenue for a while.

Cyber Essentials are effective. The assumption is they won't have been used. There is also an assumption that businesses will not pay the ransom. What is likely to happen is a mix of both.

The ransomware is not a new threat and why it is so widespread is because it is so easy to use. It is also one of the reasons why Cyber Essentials has been created and why it is so important for businesses.

Would Cyber Essentials Have Helped?

When the Cyber Essentials framework there are the security control areas. These are the foundations of good security.



Cyber extortion is a growing threat

Security industry warns of increase in attacks as Lincolnshire County Council faces ransomware demand

Warwick Ashford
 0114 270 0229
 in

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.

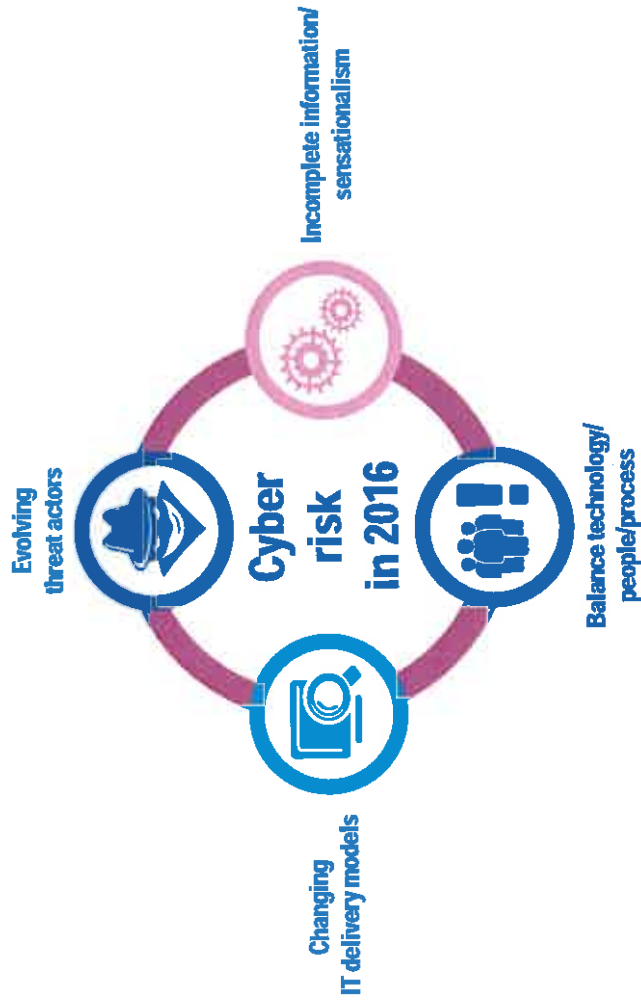


What did they do about it?

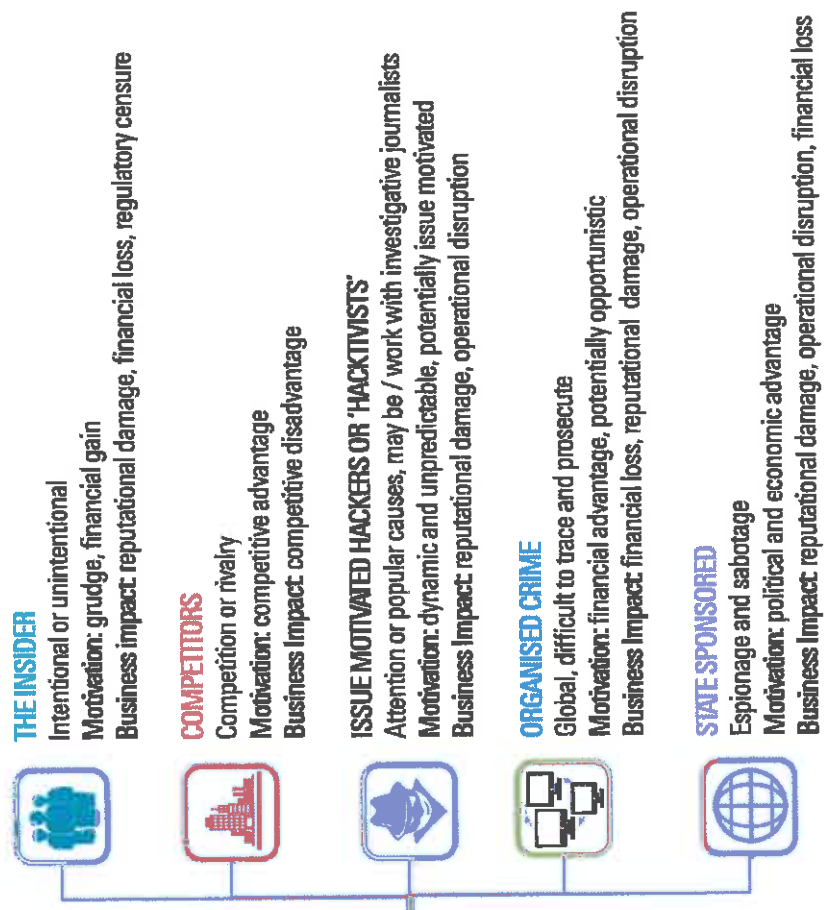
- Lincolnshire County Council acted as soon as the malware was detected preventing further damage
 - Therefore, only a small amount of their data was affected.
 - The Council had everything backed up so data affected could be restored.
- They worked with an outsourced security company to get their services 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.

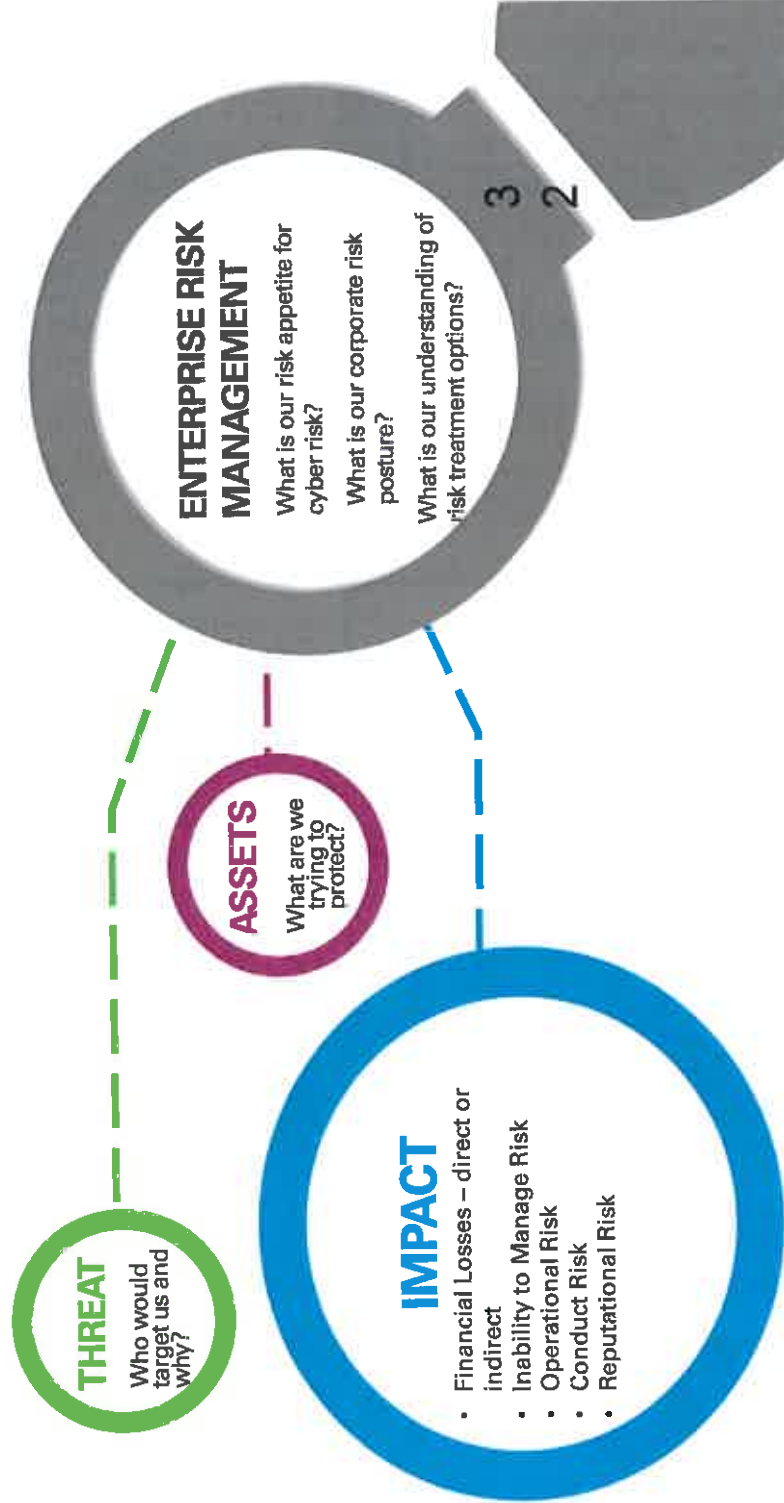
Cyber Security Landscape

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



WHO WOULD WANT TO TARGET US AND WHY?





Key Questions - Different levels

Are we a security resilient organisation?

Will future acquisitions change our security posture

The Board



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 approach 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?

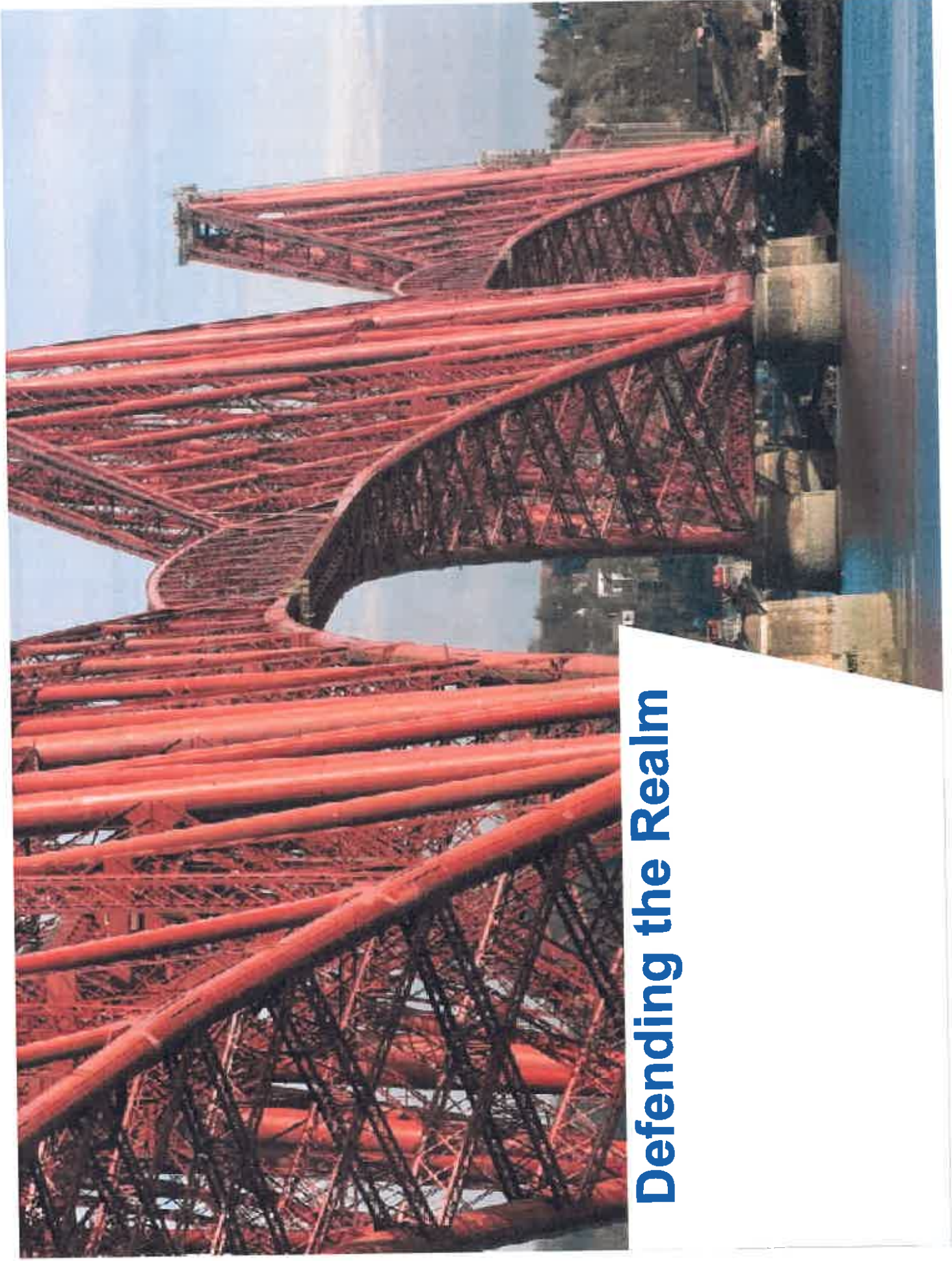
How does our security capability compare to our peers?



Head of Information Security

Am I investing in the right improvement projects?

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

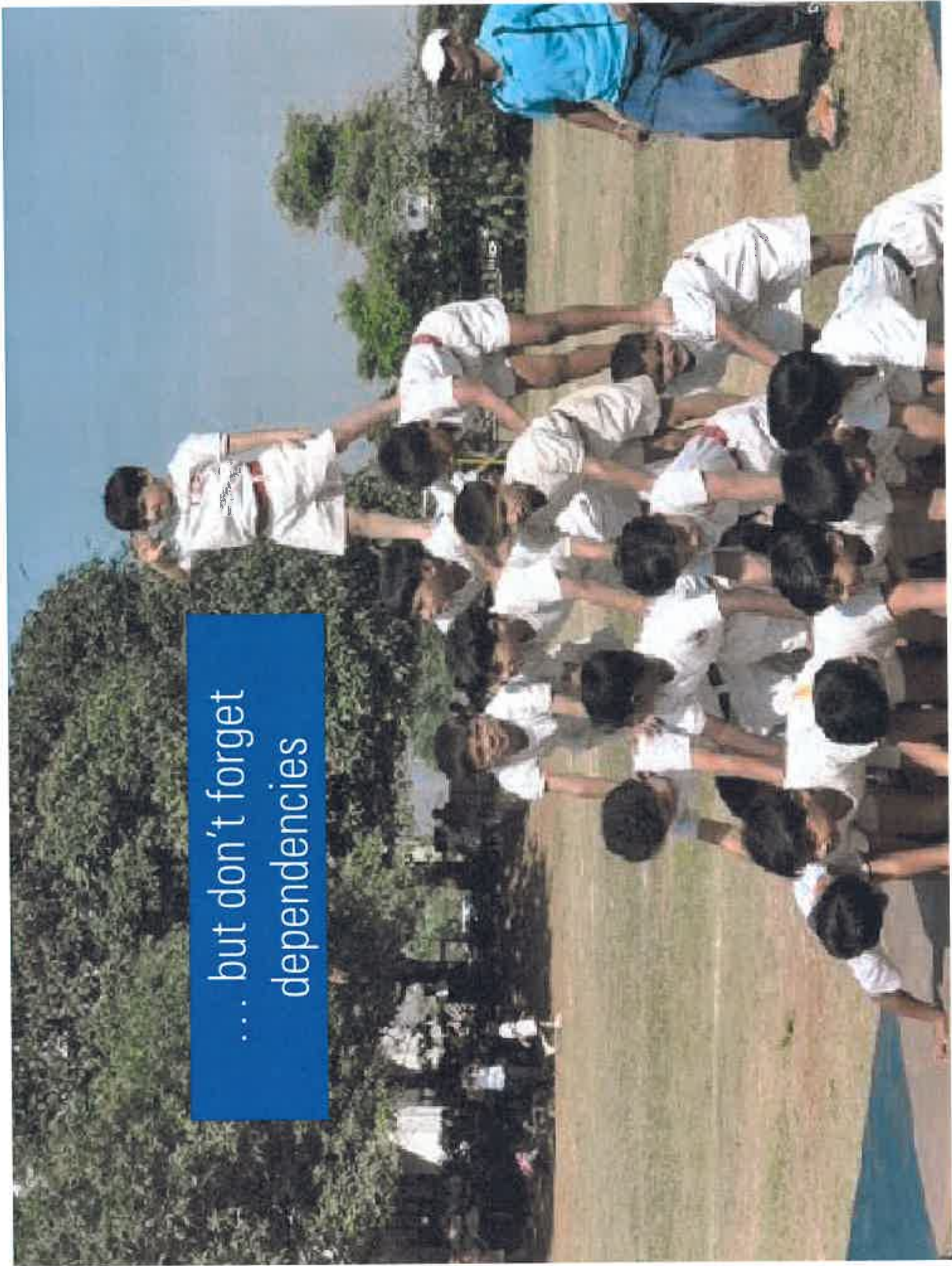


Defending the Realm

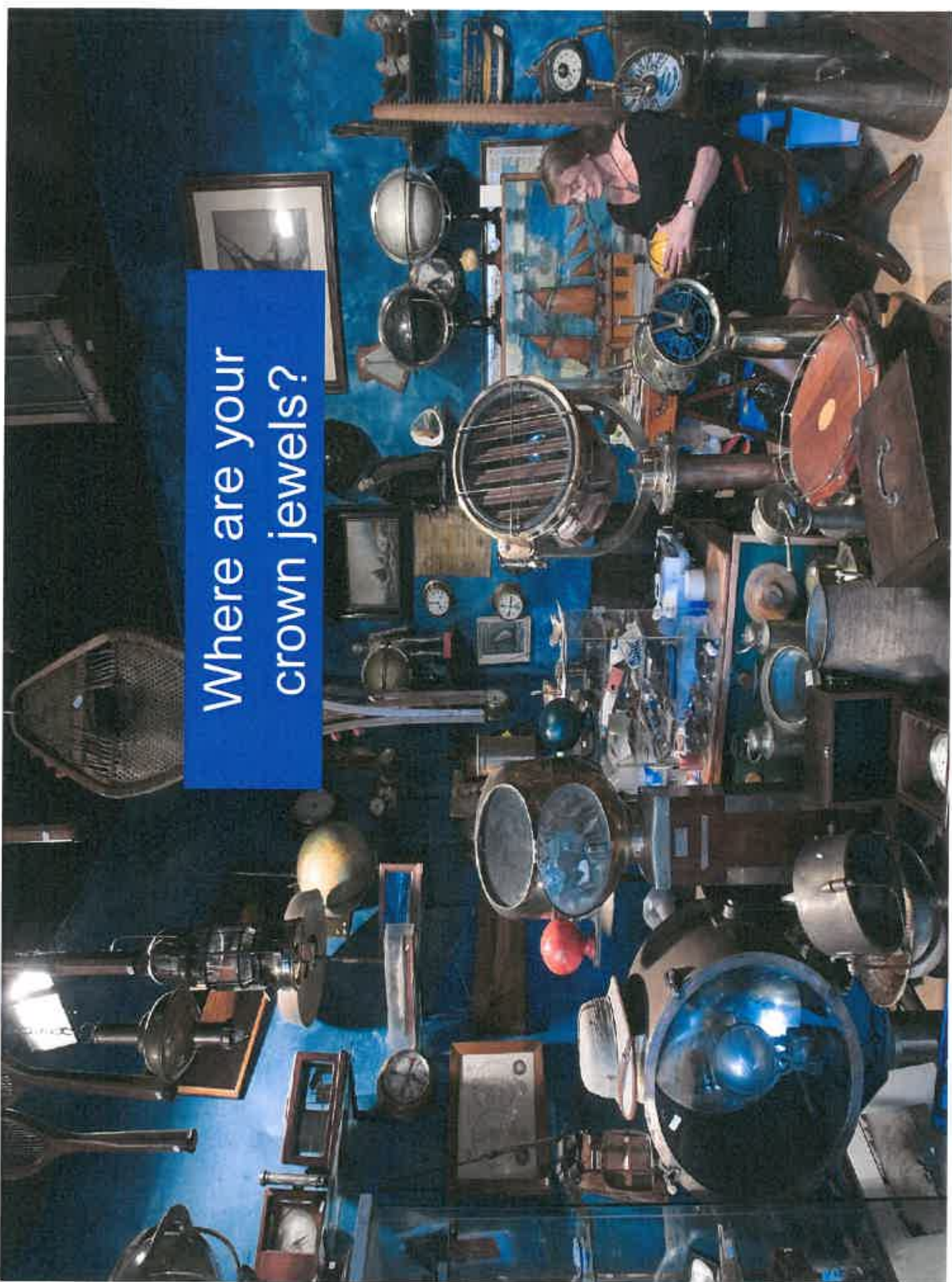
A photograph of a museum display. A large, ornate golden crown with intricate filigree, pearls, and a central blue gemstone sits on a red velvet-lined pedestal. To its right, a scepter with a long, light-colored shaft and a decorative golden headpiece stands vertically. In the foreground, another smaller golden crown is partially visible. The background is dark, highlighting the jewelry.

Know thy Crown
Jewels!

... but don't forget dependencies



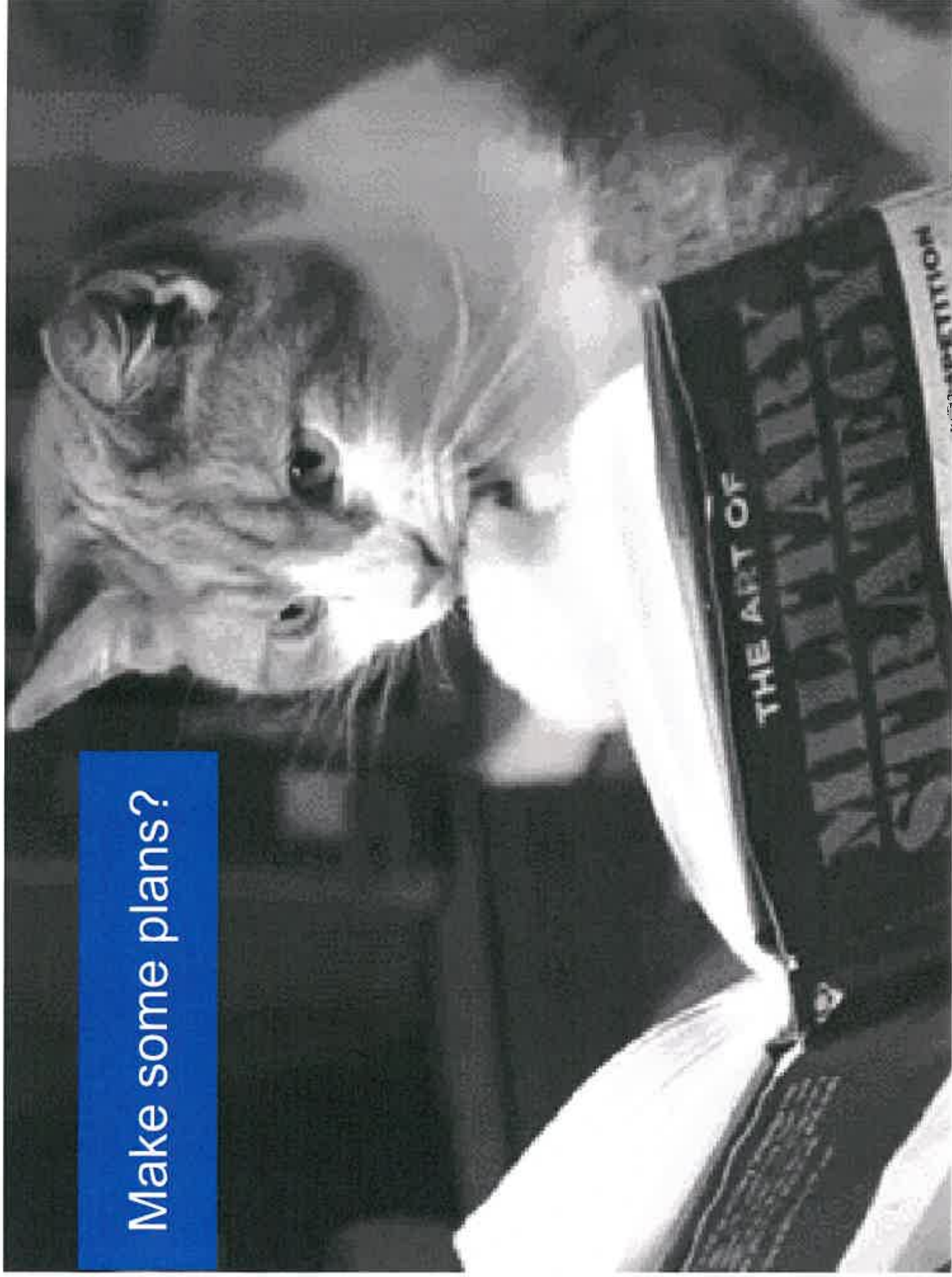
Where are your
crown jewels?



Could your crown jewels be.....

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

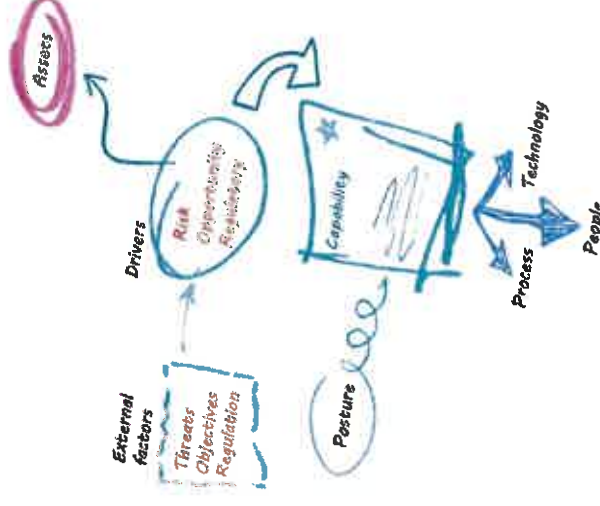
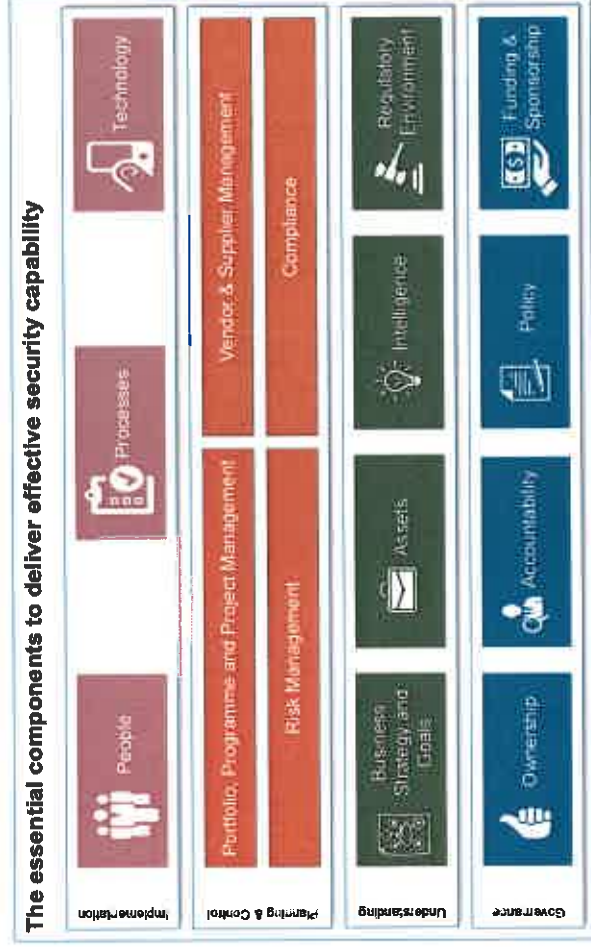
Make some plans?



Build some defences

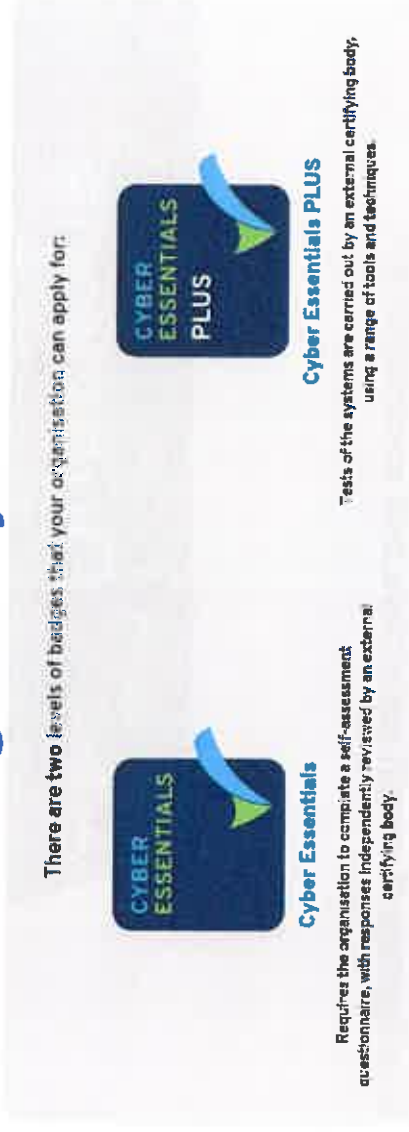


Response - How can these risks be mitigated



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

 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Co-Operative



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.

NEWS 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?





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!





The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo are registered trademarks or trademarks of KPMG International.

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

Underlying issue	Warning signals	Audit committee chair	Potential responses - Audit committee members	Management
<ul style="list-style-type: none"> Dispersing 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 	<ul style="list-style-type: none"> 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 all time to new committee members, by asking for opinions Address directly with the chairman of the board if dominance continues 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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?
<ul style="list-style-type: none"> The audit committee is being 'managed' by the executive team in attendance 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Where management team is enlightened and keen to address 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
<ul style="list-style-type: none"> 'Groupthink' - The audit committee lacks diversity of thought 	<ul style="list-style-type: none"> 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 labelled openly Different opinions or ideas not presented or evaluated 'Out of the box' thinking discouraged 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Present options and alternatives rather than a fait accompli Actively request debate when positioning difficult issues seen as hanging in the balance Overly welcome the committee's views Ensure the committee has all the relevant information to take a balanced view
<ul style="list-style-type: none"> The audit committee is overly focused on process 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Low commitment/engagement or capability of some audit committee members 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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/debats 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 	<ul style="list-style-type: none"> Insist on the maintenance of high standards Use external experience to support behavioural change 	<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Lack of reflection time about the committee's own performance, style and way of operating 	<ul style="list-style-type: none"> 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 			<ul style="list-style-type: none"> 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:



Discussion and debate is insufficient or even stifled/discouraged



Decisions are frequently presented as answers rather than options



There is over-dominance or under-contribution from certain individuals



Focus is on the quantity of areas covered rather than the quality of the discussion



The level of challenge and consideration of fresh ideas is limited



The group rarely self-reflects or accesses third parties for input

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:

[Download handbook](#)

