THE INVESTMENT ASSOCIATION

CYBER RESILIENCE

Board Engagement & Governance

Updated guidance
May 2021

Contents

Context

This document should be read in conjunction with the associated Resources Overview document, which details freely available practical steps guidance issued by regulators and members of the security community, available here.

This May 2021 version of this document is intended to update the previous version of this guidance published in 2019, to reflect new developments (particularly from the National Cyber Security Centre (NCSC)) and considerations for Boards.

As developments in cyber security are fast-moving, shaped by tech advancements and the behaviour and activity of bad actors, firms are encouraged to monitor the threat landscape on a continuous basis and adapt their approach accordingly. Members can keep up to date with IA activity and resources via our webpage.

Background

Building cyber resilience across financial services is a key priority for firms and authorities alike. The NCSC has been particularly prominent in offering a range of support and guidance for firms in this area[1]. Likewise, it remains high on the regulatory agenda and has been the focus of a number of significant regulatory publications. The pandemic and the trigger for a permanent shift to increased remote working has brought new perspectives to a subject that was already a quickly-growing item on the risk radar. The associated operational resilience discussions recently resulted in the publication of the UK authorities' regulations[2] that come into effect next year.

Firms are encouraged to adopt a 'Culture of Security' from the Board down, as it is not a case of 'if' an incident occurs, but 'when'. Cyber risk is significant and needs to be appropriately managed by adopting a threat-led approach. To build overall operational resilience across the industry it is important that all firms aim to address the FCA questions for Board members and Risk Committees on an ongoing basis. There is no end point to building cyber resilience, and firms should aim to continuously improve and enhance their cybersecurity strategies.

> Cyber security is still not taken as seriously as it should be, and simply is not embedded into the UK's boardroom thinking… In boardrooms, digital literacy is as non-negotiable as financial… literacy.
>
> Our CEOs should be as close to their CISO as their Finance Director.
>
> **NCSC CEO Lindy Cameron, March 2021**

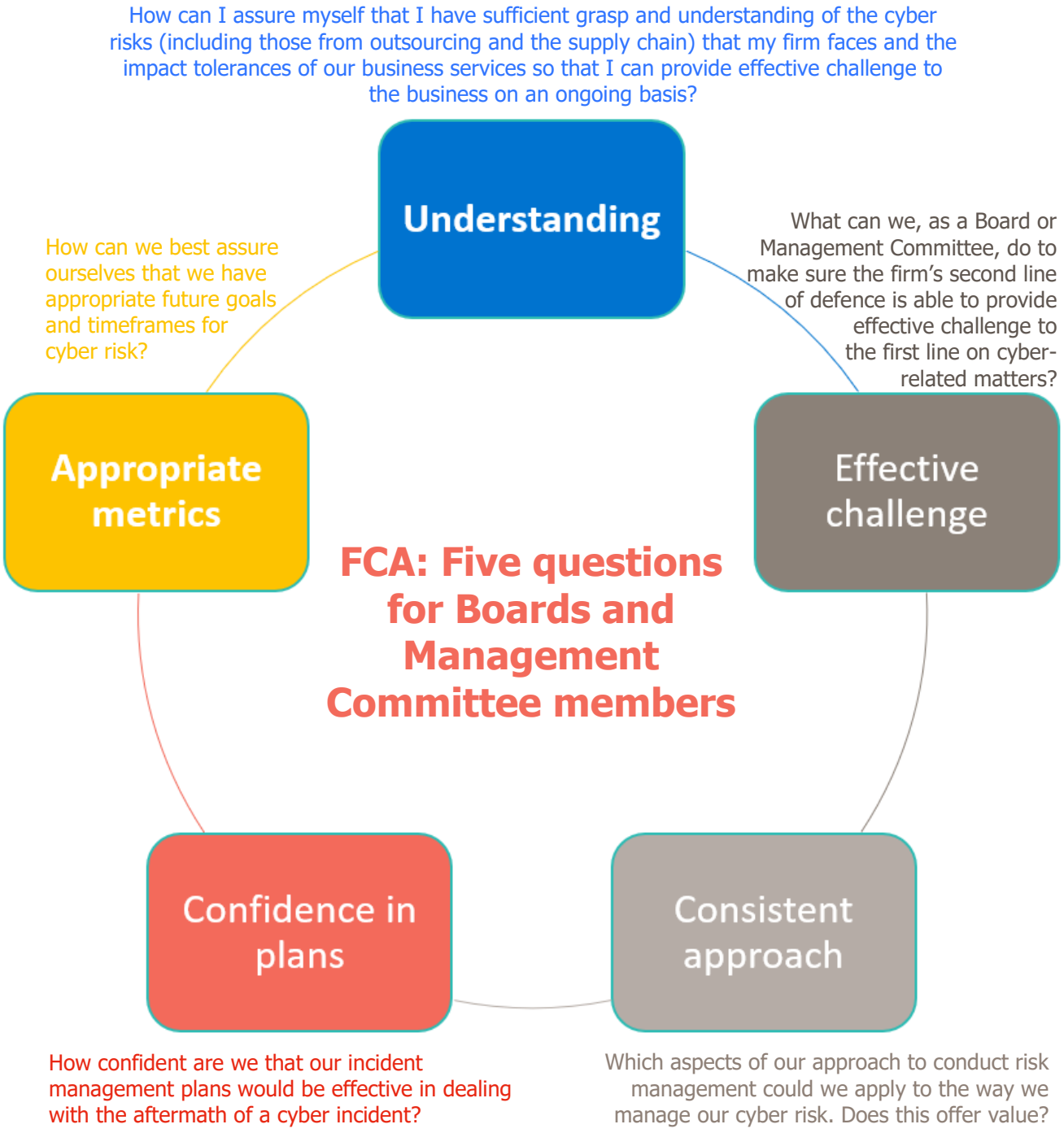
This updated document provides insight into what has worked in investment management firms in relation to the FCA's recommended questions to engage Boards and ensure appropriate governance processes around cyber resilience are in place. A supplementary Resource Overview[3] highlights additional readily available guidance which members can refer to when considering cyber risk. The key starting guidance to support Board engagement and governance can be found in the NCSC Board Toolkit[4].

---

[1] NCSC website
[2] FCA: *PS21/3 Building operational resilience*, March 2021
[3] IA: *Cyber Resilience Board Engagement and Governance Resources*, May 2021
[4] NCSC: *Board Toolkit*, March 2019

Introduction

In the FCA's wholesale banks and asset management cyber multi-firm review findings[5], the need for Boards and management to improve their understanding and management of cyber risks was highlighted as a key area of concern. To encourage meaningful and effective consideration of cyber risk, the FCA recommended five questions Boards and Management Committee members may want to ask themselves:



Guidance is detailed below on how to build good governance processes and Board engagement with cyber risk, based upon good practice occurring throughout the industry.

[5] FCA: *Wholesale banks and asset management cyber multi-firm review findings*

Key Actions

We have identified nine key actions that Boards and Senior Managers might take in order to understand their exposure to cyber risk, know their current security position, implement appropriate cyber resilience development plans and drive results.

1. Know the key threats

Board members need to understand the top cyber threats to their business in order to effectively prioritise, plan and build resilience on an ongoing threat-led basis.

Board members should also know that they themselves are a high risk target for cyber attackers. If they are not sufficiently aware or prepared they could act as a significant weak link to their firm's overall resilience and therefore need to play a key role in mitigating risk.

2. Know the important business services to identify key assets and steer investment

Board members have significant expertise in understanding their business and can therefore help to identify the firm's important business services that are critical for clients and to keep operating effectively. Identifying these deliverables and assets can help to prioritise mitigation development and implementation.

3. Know the current security position

Gaining an understanding of any current strengths and weaknesses throughout the business can help Board members to understand their firm's current maturity and begin to identify any gaps that need to be addressed. These assessments can be carried out internally or externally and should ideally be independently validated.

4. Have a clearly identified and understood set of impact tolerances

Based on the current position and important business services, impact or risk tolerances should be developed and agreed upon. Setting tolerances helps to prioritise how Boards address business risks and consider appropriate treatment options and investment implications.

5. Have appropriate cyber resilience development plans to put appropriate security measures in place

Adopting appropriate security measures tailored to the business and assets will take time and investment. Boards should ensure that a plan of action is developed that prioritises addressing key business risks. This plan needs to be regularly reviewed and revised to remain effective and take into account that a significant incident could occur at any time.

Referring to government guidance such as Cyber Essentials[6] or the NCSC 10 Steps to Cyber Security[7] can help Board members and Senior Managers prioritise actions. Certifications such as ISO 27001[8] can help to inform strategic and objective decision making.

6. Establish and endorse an information security programme

An information security programme should be established as a connected part of the overall business strategy and include setting key policies and practices that should be adopted by individuals throughout the business. People can be a huge weakness if they do not follow these policies and lack awareness of the issue.

Board members should set the tone from the top by clearly complying with and endorsing the information security programme to create a 'culture of security'.

7. Have methods in place to monitor activity and detect incidents

To maintain an ongoing understanding of activity, progress and incidents, measures should be in place to monitor activity. Identifying the root cause of an incident is necessary to address the incident in the most effective way possible.

8. Have clear reporting methods in place

As part of BAU, key indicators should be regularly reported to the Board to provide an ongoing picture of cyber resilience. A clear reporting method should also be in place in the event of an incident occurring and escalated accordingly, within the business and to the regulator and law enforcement where necessary.

9. Have tried and tested incident response plans ready

Incidents are inevitable so firms need to be ready and able to respond. A proportionate incident response plan should be in place and address not only IT disruptions, but the necessary internal and external factors such as maintaining business service delivery, communications and PR.

Regular exercising can help firms practice responding to an incident and implement lessons learned into future iterations of planning. Initial plans can be developed based on existing Business Continuity and Crisis Response Plans.

---

[6] NCSC: *About Cyber Essentials*

[7] NCSC: *10 steps to cyber security*

[8] ISO: *ISO/IEC 27001 — Information security management*

Board Member Industry Insights

Actions that Board members might take to address the FCA's 5 recommended questions.

How can I assure myself that I have sufficient grasp and understanding of the cyber risks (including those from our third parties) that my firm faces and the impact tolerances of our business services so that I can provide effective challenge to the business on an ongoing basis?

As cyber is a critical business risk, Board members must have an awareness of cyber risks and the potential impacts on their business operations.

Board Member Considerations

- To increase understanding of cyber risk and learn what you as a Board member can do to help build cyber resilience, first look at the NCSC Board Toolkit[9].
- Attending tailored cyber risk awareness training sessions and/or cyber incident simulations will increase understanding of cyber risks and the impact it has on the business.
- Attending informal sessions with relevant individuals within the firm and/or external specialists will increase understanding of what is currently happening in the firm to address cyber risk and help to identify any gaps that need to be addressed.
- Knowing the firm's key assets will increase understanding of the potential impacts of cyber risk on critical business services and allow the Board to communicate this to relevant teams to prioritize implementation of appropriate risk management processes.
- Receiving appropriate assurance on information given helps to ensure that it is accurate and that Boards are making appropriate decisions for the business.
- Treating cyber risk like any other risk to the business ensures appropriate risk management. Considering the firm's approach to existing processes, such as the ICAAP/ICARA[10], can help firms better consider and prepare for cyber risks.

What can we, as a Board or management committee, do to make sure the firm's second line of defence is able to provide effective challenge to the first line on cyber-related matters?

The first line dealing with any risk should be independently challenged to ensure that information the Board receives is trust-worthy and informative with regards to the current status of risks and areas in need of future improvement.

Board Member Considerations

- Decision makers need to be well-informed and appropriately challenged across the three lines of defence. Accountability should not be delegated to IT departments.
- Boards should encourage communication between IT, Risk and Business Service functions to improve understanding of cyber risks across the three lines of defence.
- Consider acquiring/developing IT literate talent across the three lines of defence to provide effective challenge.
- Not all firms have a clear three lines of defence. In these instances, Boards should look to independent experts to validate and challenge internal actions and reporting.

---

[9] Ibid

[10] The Internal Capital and Risk Assessment process (ICARA) replaces ICAAP in January 2022.

- It is important to receive and understand any assurance materials received from the first line of defence. An external third party assessment can help to provide assurance on cyber risk management processes and identify any significant gaps to be addressed.

Which aspects of our approach to conduct risk management could we apply to the way we manage our cyber risk. Does this offer value?

People are a key asset, but can also become a significant weakness if they do not conduct themselves in a manner that protects both the customers and the firm from cyber risk and other connected risks such as market abuse or committing financial crimes.

Board Member Considerations

- Policies, standards and processes should be in place to govern conduct risk in the risk framework.
- To manage conduct risk Boards need to ensure that a 'Culture of Security' is adopted throughout the firm. By endorsing the importance of security and showing good secure behaviour, Board members can help encourage the adoption of good behaviour throughout the firm.
- Appropriate support needs to be in place for individuals to reduce the likelihood of someone maliciously causing harm to the business and/or its customers through poor conduct. Material risk takers need to be aware of how their actions impact customer protection to understand behavioural requirements.
- Good reporting procedures must be in place to allow for the reporting of suspicious activity and ensure that any conduct issues are dealt with effectively.
- Strategic security objectives should be put in place determining the levels of Confidentiality, Integrity and Availability required for key assets. These objectives should always link back to the customer to highlight the importance of good conduct.
- Adopting these measures will put the firm in a defensible position should a lone wolf insider attack.

How confident are we that our incident management plans would be effective in dealing with the aftermath of a cyber incident?

Boards need to be ready to respond to an incident. Holistic plans need to be in place to ensure fast and effective recovery from a cyber attack and ensure that the impact is mitigated appropriately with minimal disruption to key business services and customers. Depending on the type of incident there will be legal and/or regulatory obligations that you must meet. Not responding properly and failing to meet these obligations can lead to not just significant financial loss, but reputational implications as well.

Board Member Considerations

- Boards need to set a clear statement about both their requirements and responsibilities in the future to ensure effective incident response.
- All firms need to have incident response plans that are regularly tested, updated and validated. If the resource for this is not available internally, Boards should refer to external experts. To ensure maximum effectiveness these third parties should be familiar with the business to understand how it operates and what is necessary in the event of an incident.
- A cyber incident can cause firm level disruption, so Boards can look to existing Business Continuity plans to understand requirements for cyber incident response and how this links to the wider incident framework across departments.
- Taking part in a cyber incident simulation or exercise will demonstrate the factors involved in incident response and the key decision that needs to be made. Taking part in such a scenario will provide experience and understanding that will help to develop effective incident response plans.
- It is important that Boards know the practitioners who will be involved in an incident response scenario. Steps need to be taken to make sure that everyone involved in the response process are familiar with one another and understand their designated roles.

- While a focus on the response is appropriate, Boards should take care to ensure that defensive actions are not overlooked. It is better, in many respects, to effectively prevent an incident in the first place than focus on responding to one afterwards. Investment decisions between the two areas of focus should be carefully considered to ensure budgets are apportioned appropriately.

How can we best assure ourselves that we have appropriate future goals and timeframes for cyber risk?

Developing and implementing cyber resilience development plans will take time. Firms need to make plans and set future goals that prove to the regulator that building cyber resilience is being taken seriously and that the firm is in a defensible position in the event of an incident occurring.

Board Member Considerations

- All responses and plans need set timelines. Assessments (internal and/or external) need to be carried out to ensure plans are timely and in alignment with business priorities.
- Not all future goals need to involve new technologies. Future goals can and should include getting the basics right as these measures will always be key to building cyber resilience.
- The set of goals and timeframes will show that firms and the industry have plans to improve resilience. Board members must be able to defend the proposed future goals and set timeframes in the event of an incident.
- Budget needs to be assessed to understand what investment is necessary to achieve these goals within the set timeframes whilst maintaining a competitive advantage.
- The Board need to be aware that cyber poses a unique business risk as it involves external adversaries that are constantly evolving.

Senior Manager Industry Insights

Actions that Senior Managers might take to address the FCA's 5 recommended questions.

How can I assure myself that I have sufficient grasp and understanding of the cyber risks (including those from our third parties) that my firm faces and the impact tolerances of our business services so that I can provide effective challenge to the business on an ongoing basis?

As cyber is a critical business risk, Senior Managers must have an awareness of cyber risks and the potential impacts on their business operations.

Senior Management Considerations

- Individuals communicating cyber risk to the Board should aim to do so in a way that encourages Board engagement and increases understanding to ensure informed and effective decision making.
- Firms need to consider whether the current Board membership shows sufficient willingness to engage with cyber risk.
- The Board should receive regular reports on cyber risks by a relevant senior leader in IT, Information Security, Cyber Resilience or Risk. These reports should be independently reviewed and validated to ensure that Boards are receiving useful and accurate information. External review also helps to identify gaps and provide insights as to what steps should be taken next.
- As cyber is a key operational business risk it should be treated like any other risk the Board deals with. Those presenting to the Board need to translate cyber risk into business language. This could include incorporating cyber risks into existing risk registers and/or addressing cyber risks in commonly used risk reporting processes, for example, ICAAPs/ICARA[11].
- Providing Boards with tailored awareness training will build understanding of cyber risks and add context to enable better informed decision making. To get the message across quickly to senior individuals, Senior Managers can consider sharing informative videos or performing exercises such as those highlighting personal social media risks or table-top exercises as provided by Cyber Griffin[12].
- Provide informal sessions with interested Board members to facilitate discussion and ask questions. Including real-world examples and wider business context can strengthen the narrative and better engage Boards with the issue.
- Mapping business processes and associated cyber risks and controls can help to provide the Board with a fuller picture of assets, threats and business impact.
- To communicate key risks, it may be helpful to provide Boards with a more detailed presentation on that hot topic to ensure they have sufficient understanding to support their decision making.
- Hosting practice exercises and/or cyber incident response simulations will bring the issue to life and provide the Board with valuable context and understanding of the importance of cyber resilience.
- Once Boards have identified risk tolerances for key business services, the critical assets supporting each of those services should have set requirements regarding Confidentiality, Integrity and Availability.

What can we, as a Board or management committee, do to make sure the firm's second line of defence is able to provide effective challenge to the first line on cyber-related matters?

[11] The Internal Capital and Risk Assessment process (ICARA) replaces ICAAP in January 2022.

[12] Cyber Griffin website

The first line dealing with any risk should be independently challenged to ensure that information the Board receives is trust-worthy and informative with regard to the current status of risks and areas in need of future improvement.

Senior Management Considerations

- With the implementation of SM&CR, Senior Managers should ensure that someone is responsible for cyber resilience and has sufficient understanding to hold responsibility for managing cyber risks.
- Communication between Risk, IT and Business function is crucial to ensure appropriate understanding and challenge.
- Any metrics/statistics provided to the Board need to be meaningful and clearly demonstrate the impact of an incident and/or the effectiveness of controls. For example, firms may wish to share the overtime necessary to deal with an incident rather than complex technological control statistics.
- Providing some consistent key risk indicators (KRI)'s and gap labelling using, for example, red-amber-green classification, can act as clear signals to the Board on what is working, what is not and how to prioritise.
- Not all firms have three clear lines of defence. If firms do not have the capability internally to challenge actions and information provided by the IT team, Senior Managers should look to get this reviewed by a trusted third party. It is recommended that support should come from accredited third parties, for example, those who are CREST accredited.

Which aspects of our approach to conduct risk management could we apply to the way we manage our cyber risk. Does this offer value?

People are a key asset, but can also become a significant weakness if they do not conduct themselves in a manner that protects both the customers and the firm from cyber risk and other connected risks such as market abuse or committing financial crimes.

Senior Management Considerations

- Senior Managers need to get the message through to their teams about the importance of practising basic cyber hygiene and conducting themselves in a manner that supports the information security programme. This can be achieved by being seen to put these good behaviours into practice and maintaining awareness and engagement throughout the team.
- Encouraging individuals to report suspicious behaviour and having an effective and supportive reporting process in place will help monitor and manage conduct and any associated cyber risks.
- Measures taken to prevent conduct risk in areas such as market abuse and financial crime should be considered and adapted to address cyber insider threats.
- If anyone notices individuals not complying with security requirements, discussions should be had to understand why they are taking potentially harmful action. Based on this discussion, security measures should be revisited to improve messaging and culture to discourage this behaviour or adapt the measure to ensure sufficient security of key assets whilst still enabling critical business services.
- Senior Managers can use conduct risk and culture based awareness and training programmes to inform how best to develop such programmes to address cyber risk.

How confident are we that our incident management plans would be effective in dealing with the aftermath of a cyber incident?

Boards need to be ready to respond to an incident. Holistic plans need to be in place to ensure fast and effective recovery from a cyber attack and ensure that the impact is mitigated appropriately with minimal disruption to key business services and customers. Depending on the type of incident there will be legal and/or regulatory obligations that you must meet. Not responding properly and failing to meet these obligations can lead to not just significant financial loss, but reputational implications as well.

Senior Management Considerations

- Senior managers need to ensure the Board are aware of any legal and/or regulatory obligations associated with incident responses and communicate these when discussing response plans with the Board.
- Businesses and regulators want to know the root cause of an incident for investigative purposes and to inform future preventative measures. It is necessary to monitor systems and hold appropriate logs for a period of time that will provide useful records and evidence in the event of an incident. These logs should be used to inform decision making on implementation of future security measures.
- Links need to be made between teams across the business who will need to be involved in the event of an incident. This includes business functions, PR, legal and communications. Plans need to be developed using a holistic approach and should be clearly communicated and understood by all individuals involved. These roles should be clearly stated in any incident response documentation.
- If sufficient capability to deal with an incident is not available internally, external specialists need to be involved to provide that necessary resource when you need it.
- Both internal and external communications in the event of an incident need to be planned and coordinated to reduce the potential cyber and reputational risks associated with miscommunication.
- A playbook for incident response is nothing without the protection steps that they require.

How can we best assure ourselves that we have appropriate future goals and timeframes for cyber risk?

Developing and implementing cyber resilience development plans will take time. Firms need to make plans and set future goals that prove to the regulator that building cyber resilience is being taken seriously and that they are in a defensible position in the event of an incident occurring.

Senior Management Considerations

- Having designated Senior Information Risk Owners and Information Asset Owners ensures that information assets are appropriately managed. This oversight can help to provide the Board with insights on current security positioning throughout the firm to help inform the development of plans and setting timeframes for key goals.
- Utilising threat intelligence will inform what upcoming threats and vulnerabilities should be addressed by when. A risk-based approach should be taken to help prioritise addressing any current gaps.
- Benchmarking the firm's current position will provide important insight to understand where goals should be directed to ensure that firms are at the right level of maturity to be resilient and maintain a competitive advantage.
- A set of metrics to be reported to the Board on an ongoing basis. These should be selected to demonstrate criticality of threats and capability to address these threats to inform Board decision making.

Additional Resources

Further detail and additional resources can be found in the Cyber Resilience Resource Overview: Board Engagement & Governance.

Also of interest may be the IA's recent report with EY on the Effective Governance of Operational Resilience, in the context of the new UK operational resilience rules which come into effect in March 2022.

The Investment Association

Camomile Court, 23 Camomile Street, London, EC3A 7LL

www.theia.org

Business: Risk, Culture & Resilience

@InvAssoc @The Investment Association