Supply chain cyber security

Managing a supplier assessment and oversight programme

19 October 2022

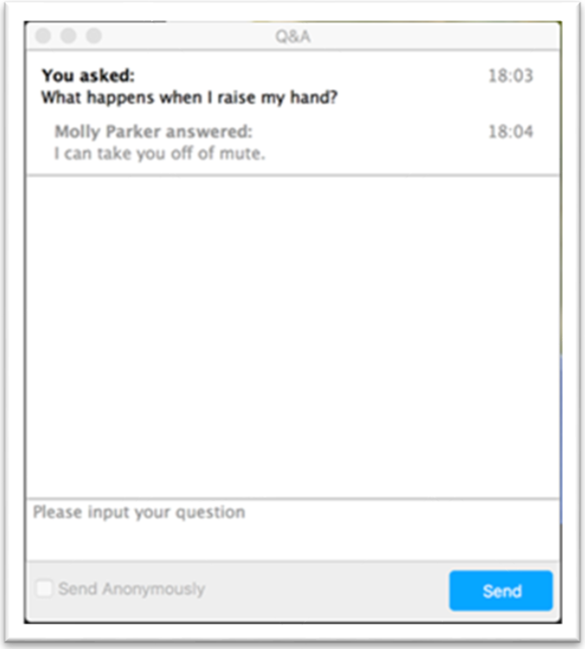
Presenters: Maritz Cloete and Richard Jackson, Moore ClearComm

Today’s presenters

Maritz Cloete
Director, Cyber Security & IT Assurance Services
MooreClearComm

Richard Jackson
Partnership manager
MooreClearComm

Ask a question



You asked: 18:03
What happens when I raise my hand?

Molly Parker answered: 18:04
I can take you off of mute.

Click on the Q&A button in the bottom toolbar to open the submit question prompt.

Type in your question and click send.

Note. If you wish to ask anonymously tick the send anonymously box shown on the illustration to the left.

Supply chain cyber security webinar series

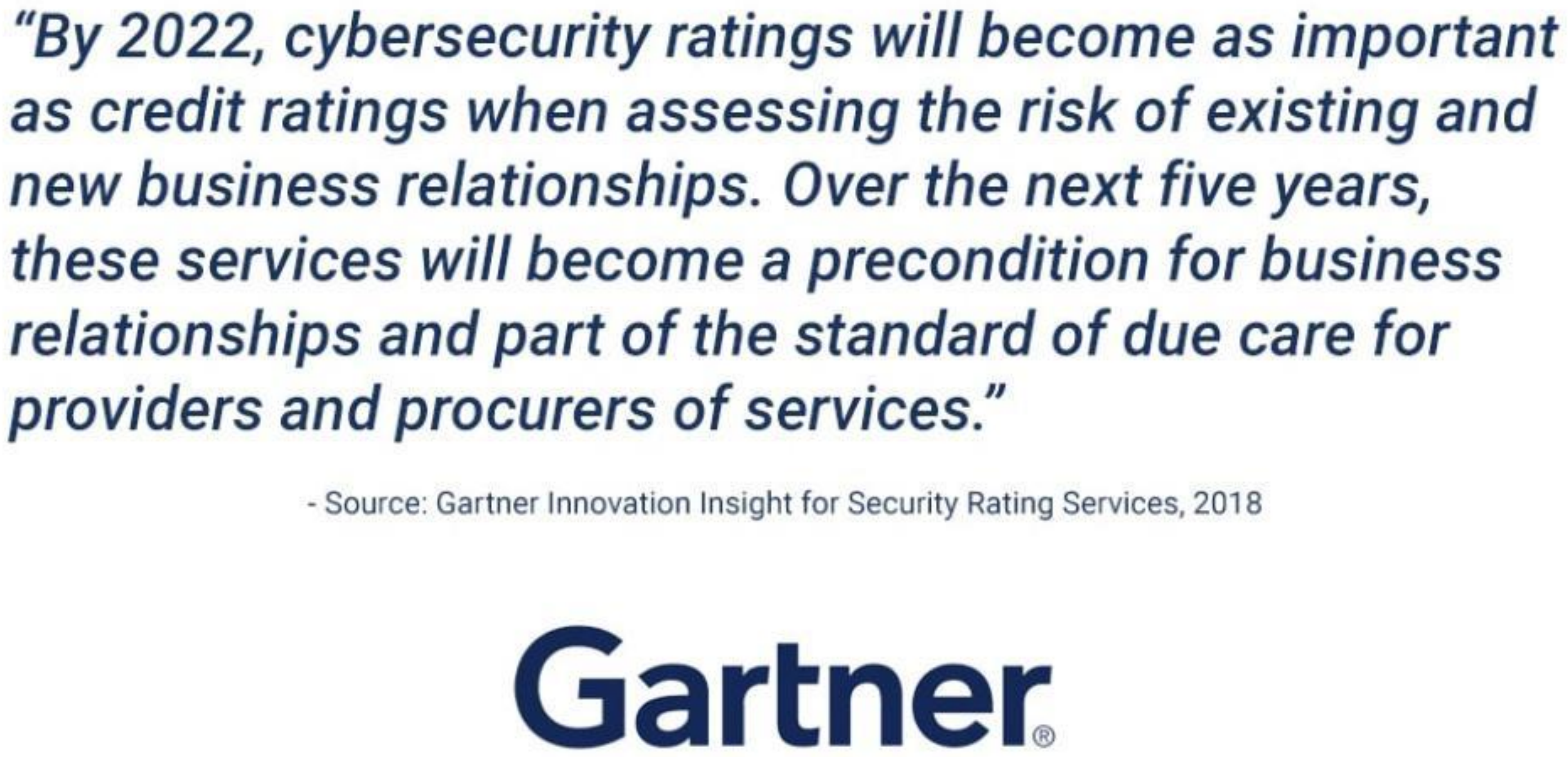
02 Nov: Recap and question and answer session

- **https://events.icaew.com/pd/25435**

Recordings available

- 28 Sep: Introduction session
- 05 Oct: Understanding the risk that your supply chain poses to you
- 12 Oct: Embedding security in agreements

- **Icaew.com/techwebinars**



> “By 2022, cybersecurity ratings will become as important as credit ratings when assessing the risk of existing and new business relationships. Over the next five years, these services will become a precondition for business relationships and part of the standard of due care for providers and procurers of services.”

- Source: Gartner Innovation Insight for Security Rating Services, 2018

Gartner®

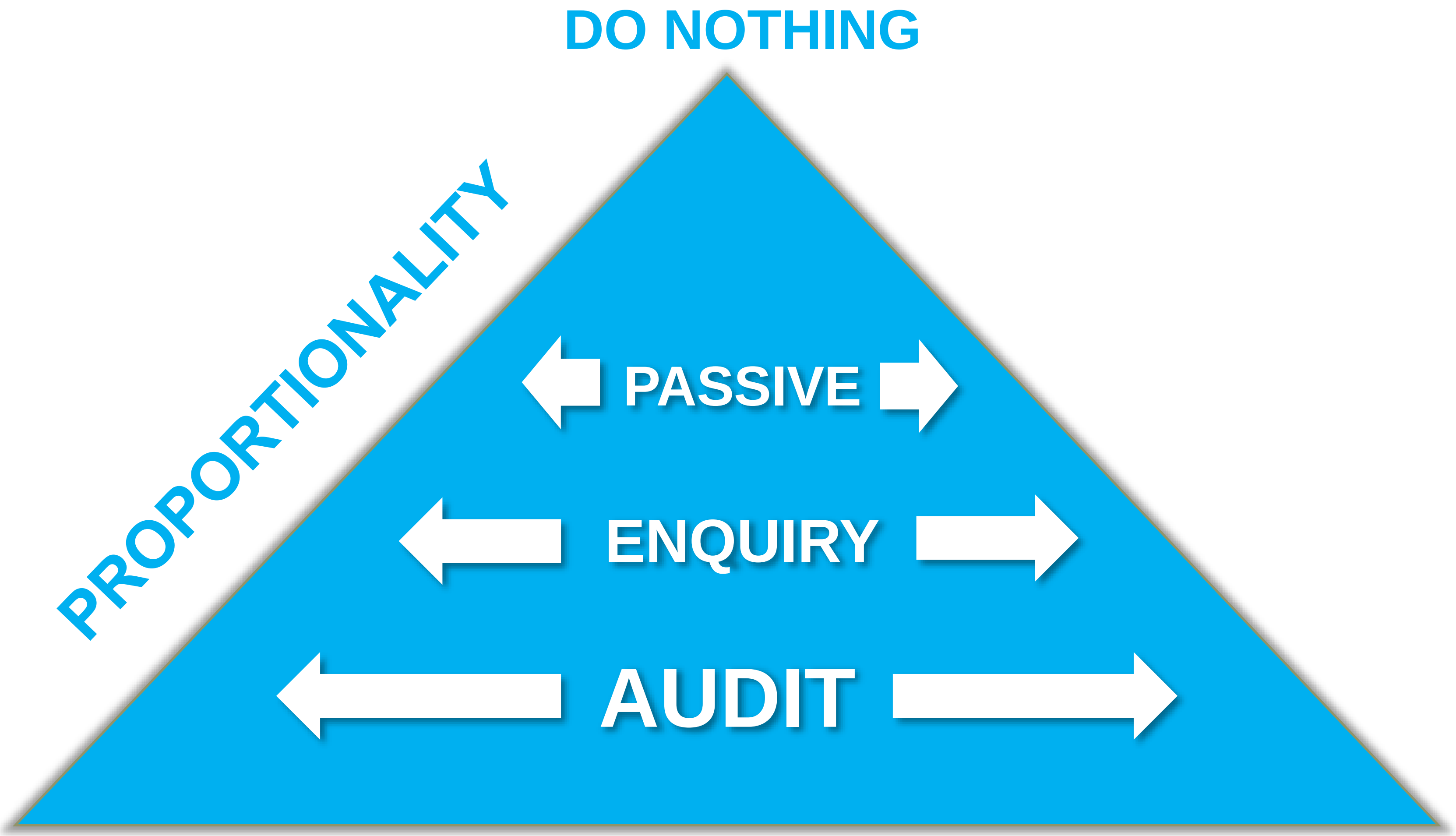
MOORE ClearComm

Managing a Supplier Assessment and Oversight Programme:

Four Stages of Assurance

MOORE Clear Comm

Four Stages of Assurance:



MOORE Clear Comm

Passive

- Taking an external view of your supplier
- Checking publicly available resources for evidence of security commitment and focus
- Renewals of annual frameworks such as Cyber Essentials, Cyber Essentials Plus and ISO 27001
- Lapses in renewal – what might this indicate?
- Access and review of 3rd party audits of your supplier

Enquiry

- The next step from “Passive”
- Ask questions of your supplier
- Ensure the questions are open, and generate qualitive responses
- Communicate “Why” you are asking these questions, and explain the objective
- Engage the services of an external provider, if you do not feel you have adequate in-house resource to manage and understand the process

Enquiry: Example Questions

- Does the organisation have a formal vulnerability management policy in place?

- What is the approach to applying operating system and security updates to the systems user to provide services to you?

- Do they carry out periodic external and internal security vulnerability or penetration tests?

- If so, when was the last test carried out, and what was the scope of the test?

- How do you ensure (our) sensitive information is transmitted to and from your organisation securely?

Audit

- May not be necessary with some/any of your suppliers (think – Proportionality)

- Intensive review of your suppliers processes and approach to cyber security and data protection

- Permission unlikely to be granted by your (larger) mainstream suppliers

- Requires expertise and likely not a persona within mid-small-sole trader firms

- Demands: Labour, Time, Resource, Skills and Commitment to maintaining audits year on year

Final Stages

- Improvement Plan

- Passive, leading to Enquiry

- Enquiry, leading to Audit

- Risks for YOU to Manage and / or Mitigate

- Core Action: Retain or Change supplier, based on:

a) What they perform on your behalf
b) The nature of the data and activity
c) Risk and Proportionality
d) Supplier Appetite for Improvement
e) Your Leverage with Supplier

Thank you for attending

Please take the time to fill out our short survey

Phone: +44 (0)20 7920 8526
Email: faculties@icaew.com

richard.Jackson@mooreclear.com

www.moorclear.com

@MooreClear

Moore ClearComm