

The CISO Share Approach to CYBERSECURITY and TTX

CISG AND PCMG ANNUAL CONFERENCE:

NO GOING BACK: TRANSITIONING TO A HYBRID WORKPLACE

CISO-SHARE – DAVID LOWE-ROBERTSON

CISO-SHARE – STEVEN MCINTOSH

Who are HEFESTIS and CISO Share?

Non-profit IT consulting and services agency working from and with the Higher and Further Education sector in the UK

CISO-Share currently works tirelessly on improving cyber security

Collaboration with Government and expert partners

The background of the slide is a collage of five blue-tinted photographs of various university buildings and campuses. The images are arranged in a grid-like fashion, with some buildings appearing in multiple panels. The overall tone is professional and academic.

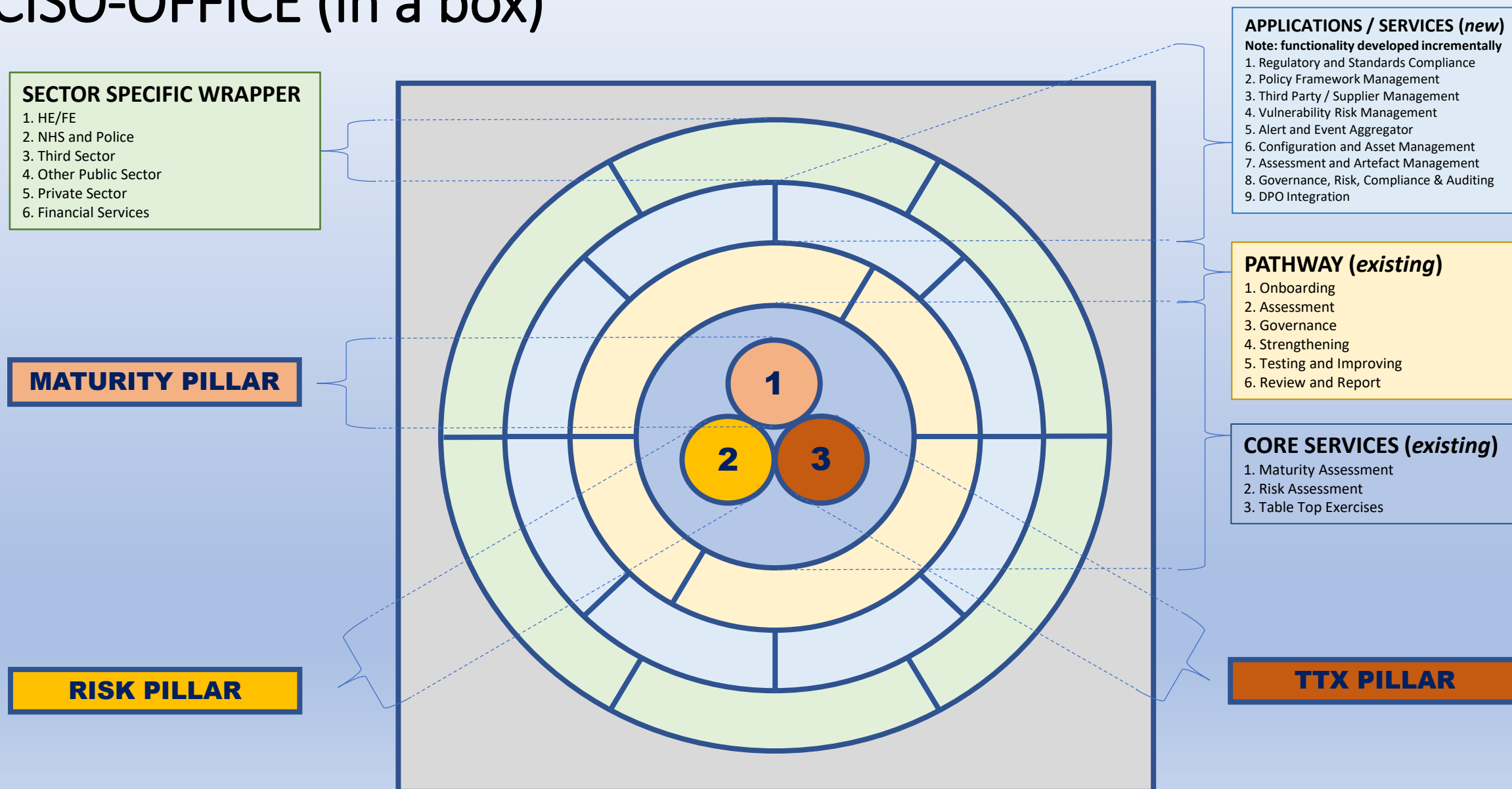
Why are we here?

Risk and consequence of Cyber attack keep on rising
Not all Universities and Colleges can afford to build the
teams, skills and services they would like

We deliver a shared service to provide dedicated cyber
security support at significantly reduced cost

Growing and active member community

CISO-OFFICE (in a box)



The Pathway : 7 Steps Of Engagement

Induction – identifying where each organisation is with cyber-security

Introduction – adopting/adapting information security and risk working groups

Engagement – working with the groups and stakeholders to manage cyber security throughout the organisation

Baselining – populating action plans, risk and maturity assessments

Strengthening – prioritising specific areas for improvement

Workshops and reviews– recording improvement, with deeper dives into specific areas where there may be gaps

BAU, continuous improvement, security by design, (Annual) Reporting on maturity and risk to the PSAP and national standards etc.





Table Top eXercises

Why do Table Top eXercises?

Advantages

- Low stress environment
- Low cost
- Ongoing evaluation
- Facilitated group discussion of problem areas

Disadvantages

- Can lack realism
- Not a true test of operational capability

An isometric illustration of a staircase made of grey blocks, with a few blocks at the bottom being red. Various stylized human figures are positioned on the blocks, some standing, some sitting, and some using devices like laptops and smartphones. The background is a dark grey gradient.

How do you
run them?

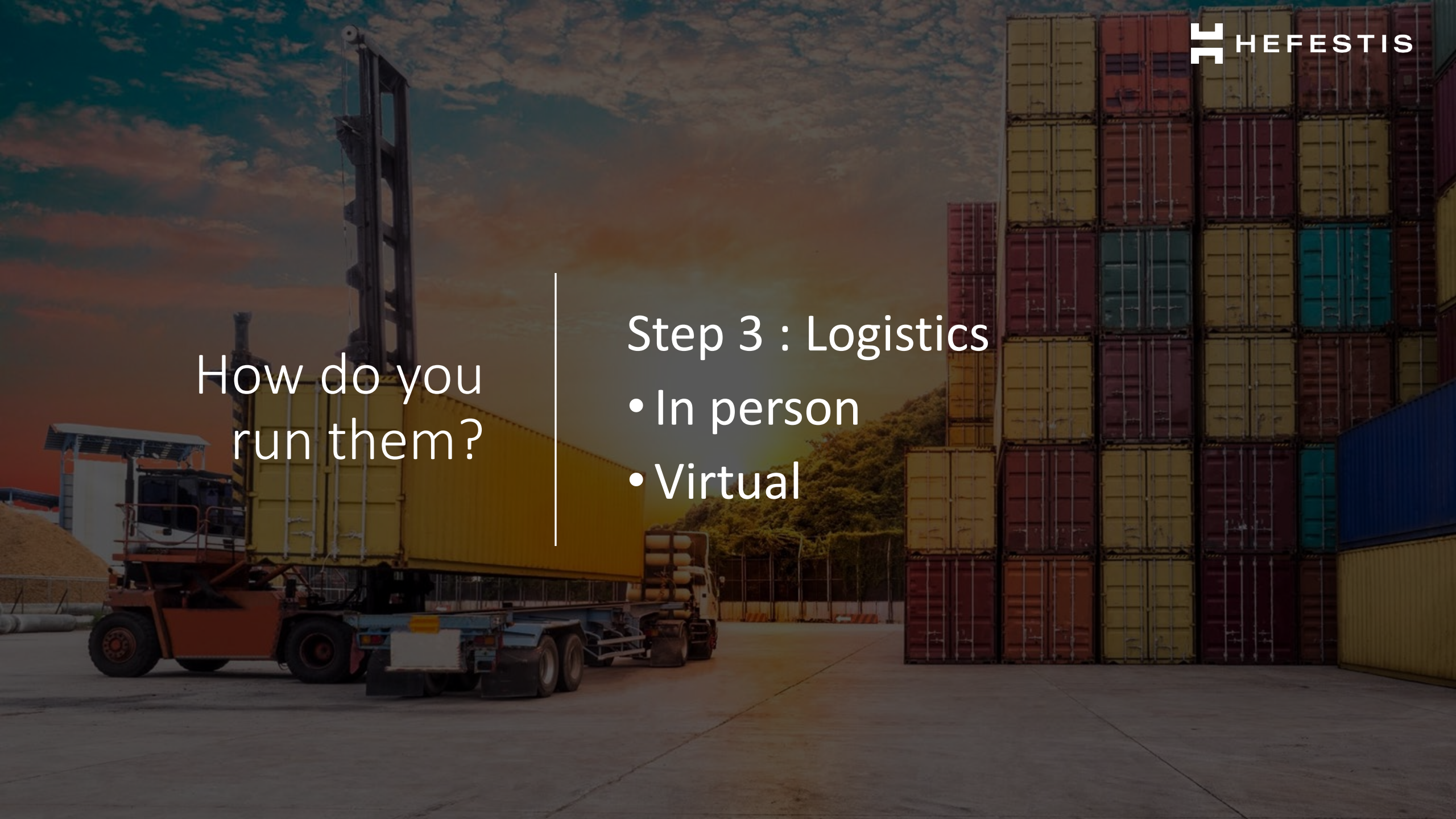
Step 1 : Audience

- Strategic
- Tactical
- Operational

How do you run them?

Step 2 : Set Objectives and Outcomes

1. Determine the effectiveness of cyber training provided to staff
2. Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment
3. Test effectiveness of the organisation's incident response plans Basic
4. Test the effectiveness of communications processes during an attack
5. Test the organisation's capability to determine operational impacts of cyber-attacks and implement proper recovery procedures
6. Enhance cyber awareness, readiness, and coordination
7. Expose and correct weaknesses in cyber security systems, policies and procedures
8. Test ability to detect and properly react to hostile activity
9. Understand the implications of losing access to IT systems and test the workarounds for such
10. Develop contingency plans for surviving the loss of some or all IT systems



How do you
run them?

Step 3 : Logistics

- In person
- Virtual



Questions