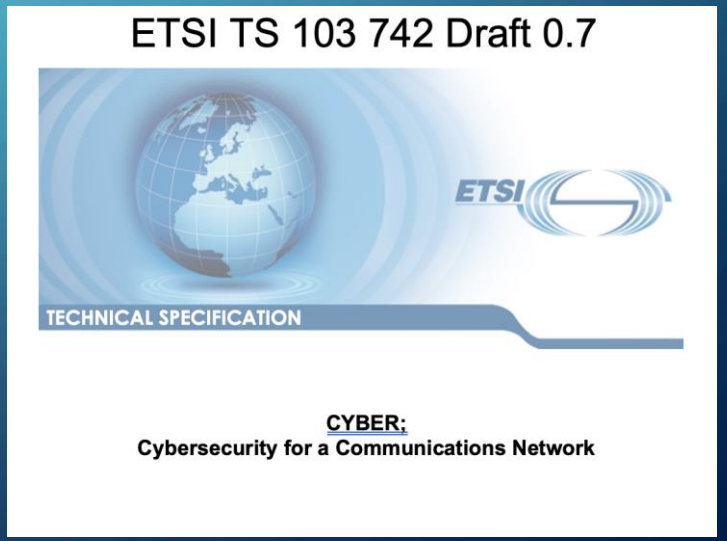
ETSI TS 103 742 DRAFT 0.7: CYBERSECURITY FOR A COMMUNICATIONS NETWORK

CHARLES BROOKSON OBE CENG FIET FRSA

RAPPORTEUR *FOR THIS ITEM* IN ETSI TC CYBER

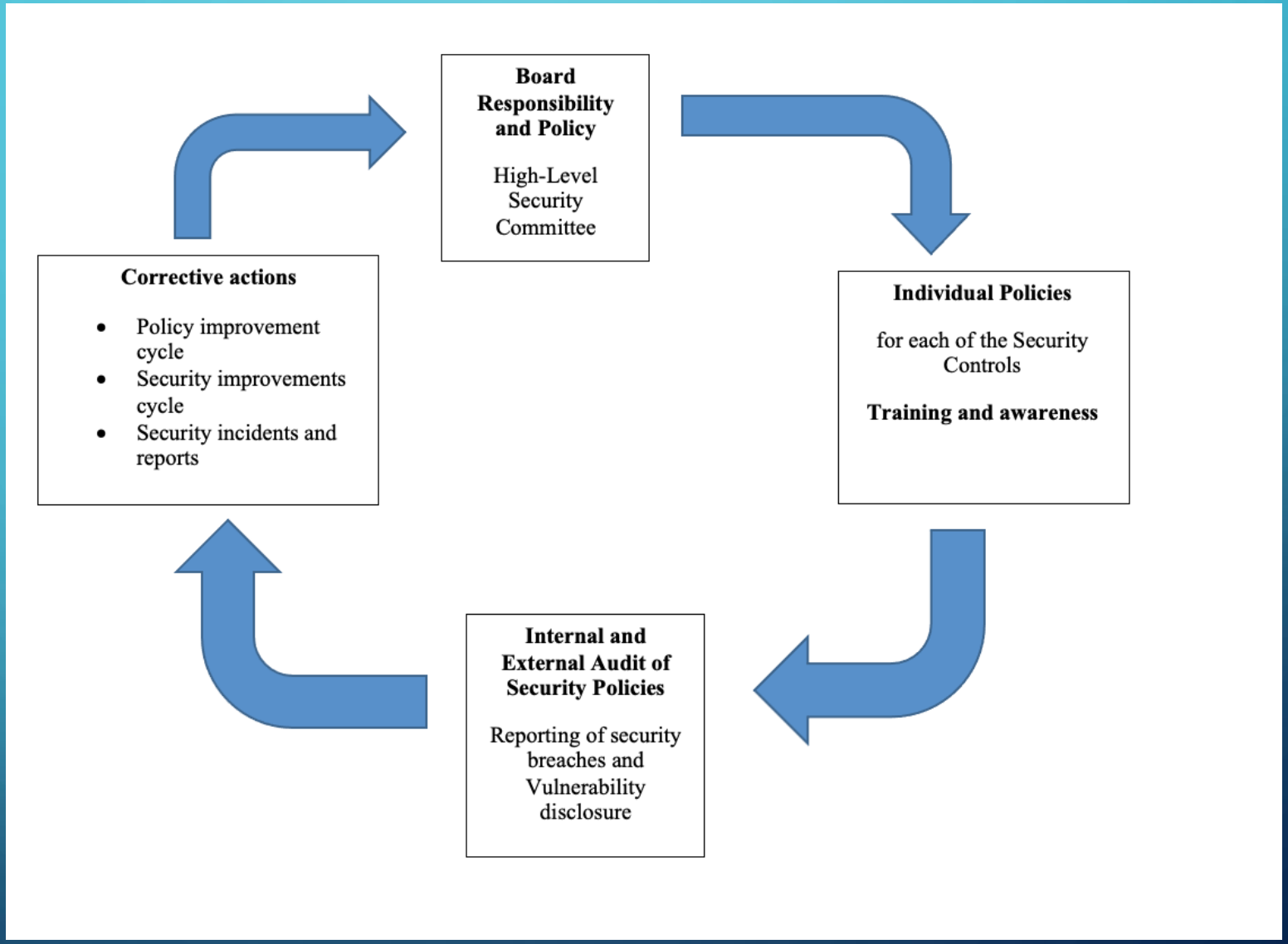
ZEATA SECURITY LTD



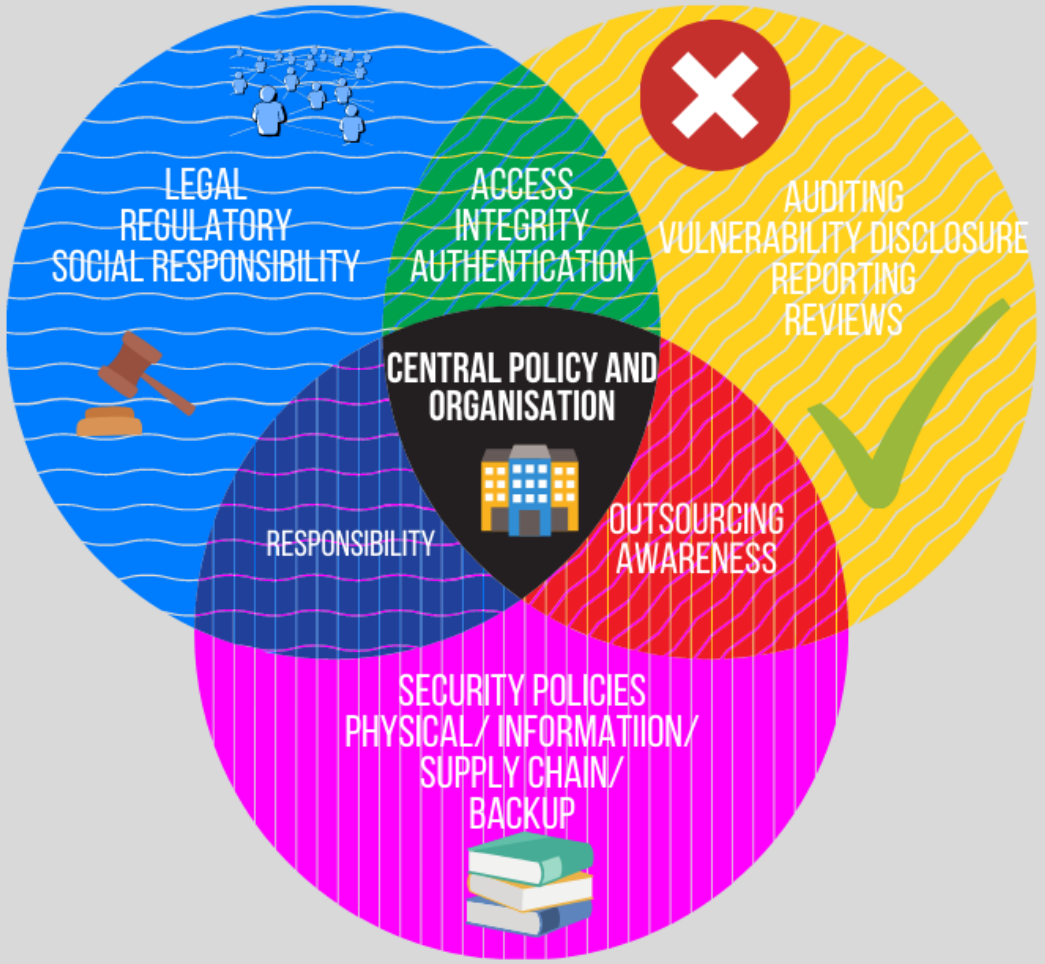
MOTIVATION

- Lots of examples 5G toolbox, ENISA, GSMA FS.31
  - National and International examples
- Need something:
  - Very simple to ensure security is addressed, which is free to everyone
  - Applicable to all Communications: SME, Corporate, Mobile, MVNO, Fixed, Wireless
  - Detailed guidance can be added for each sector *at a later date*
- At present a TS, could be made an EN (enhanced Status) (like ETSI IoT EN)

POLICY CYCLE



BASIC POLICIES



POLICIES 1- 8

- Policy 1 - A Security Policy shall exist for the **organisation, with a supporting management structure, with appropriate controls**
- Policy 2 - A Policy shall exist for the **storage of the security related data and information.**
- Policy 3 – A Policy shall exist for the **security of sensitive information and key management.**
- Policy 4 – A Policy shall exist for **personal information, as defined by local legislation, and give the consumer the ability to opt-in, consent and withdraw.**
- Policy 5 – A Policy shall exist for **signalling integrity and protection.**
- Policy 6 – A Policy shall exist for **software and virtual functions with a risk assessment, and explicit security countermeasure identified, and mitigation included.**
- Policy 7 – A Policy shall exist for **security back up and contingency planning, and it should be regularly tested.**
- Policy 8 – A Policy shall exist on the **security of outsourcing of infrastructure and services.**

POLICIES 9 - 17

- Policy 9 – A Policy shall exist **to secure the physical security and management of SIM and eSIMs and Tokens.**
- Policy 10 - A Policy shall exist for the **Physical security of assets and infrastructure.**
- Policy 11 – A Policy shall exist to ensure **Supply chain security.**
- Policy 12 - A Policy shall exist **for Co-ordinated Vulnerability Disclosure scheme.**
- Policy 13 – A Policy shall exist for **regular security testing and auditing.**
- Policy 14 – A Policy shall exist for the security of **access, password, accountability of monitoring and auditing.**
- Policy 15 – A Policy shall exist for **fraud detection and minimisation of risks for a public operator and consumer.**
- Policy 16 – A Policy shall exist for **legal conformance.**
- Policy 17 – A Policy shall exist to ensure **security training and awareness.**

THANK YOU

feedback welcome to my email charles@zeata.co.uk