DIGITAL TELECARE SECURITY ASSESSMENT SCHEME

Andy Grayland, Chief Information Security Officer, Digital Office for Scottish Local Government

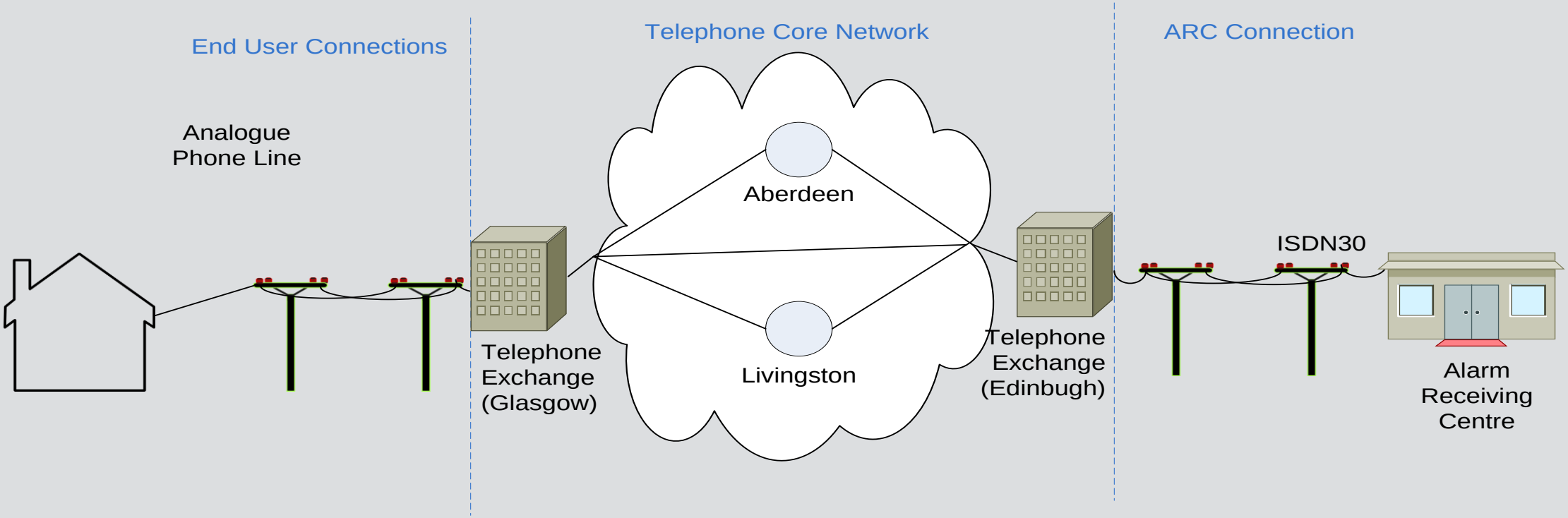
STRUCTURE OF PRESENTATION

- Overview of issue
- The security of digital telecare
- Our experimental solution
- Outcomes
- Recommendations

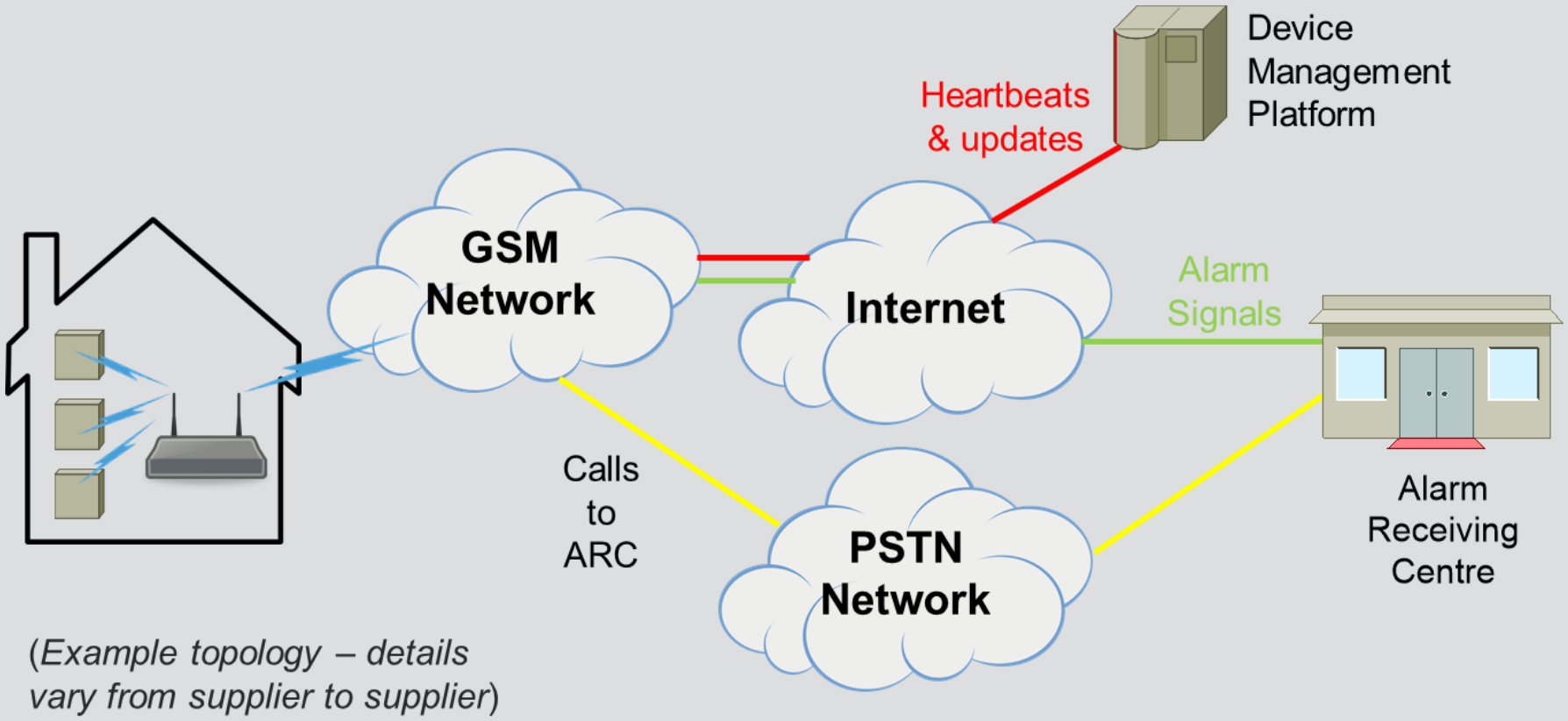
OVERVIEW OF ISSUE

- Supplier security is a major risk
- DPA 2018 – shared responsibility
- Councils will be held accountable for failures, not suppliers
- Individual customers have little sway over suppliers' security
- Niche markets do not allow for market forces to drive change
- Suppliers can often be unaware of the standard they need to achieve

DIGITAL TELECARE- ANALOGUE LEGACY

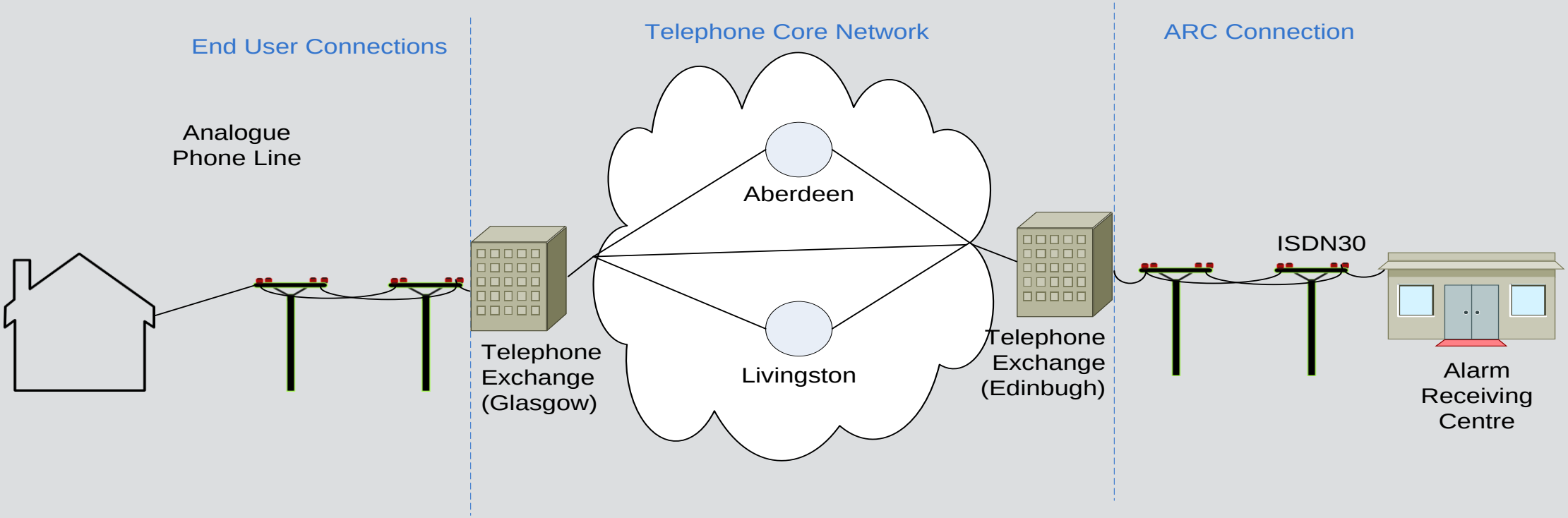


WHAT'S CHANGED - DIGITAL



(Example topology – details vary from supplier to supplier)

WHY DOES IT MATTER - ANALOGUE



DIGITAL OFFICE
Scottish Local Government

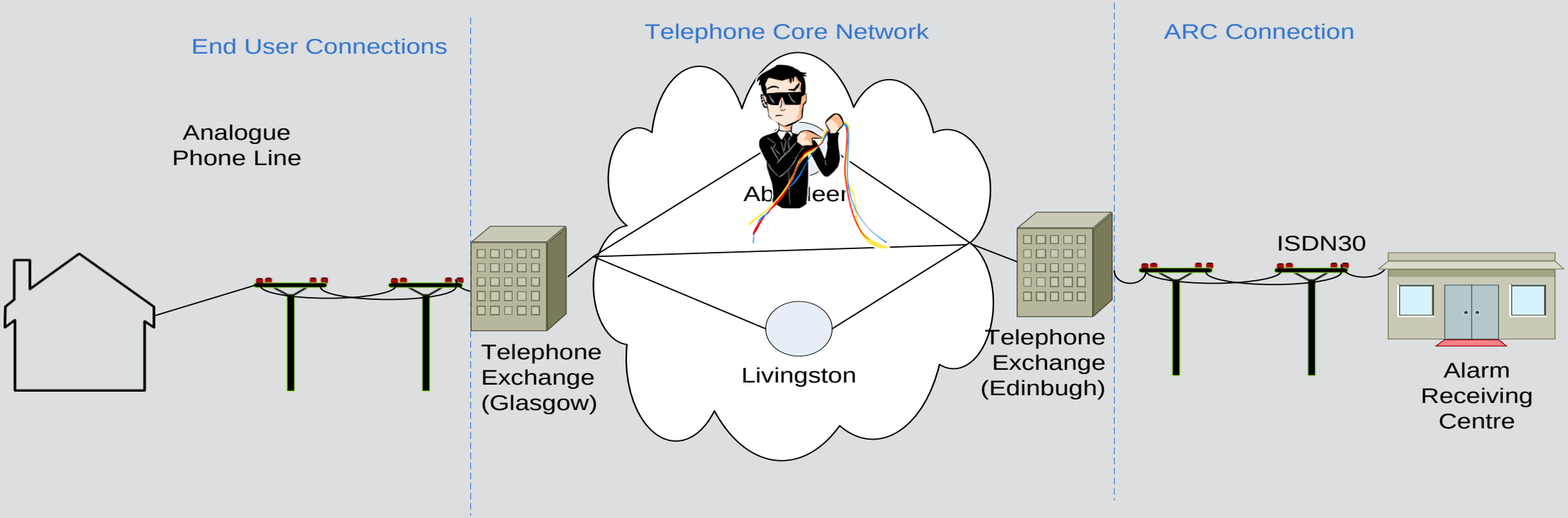
TEC Technology Enabled Care

Scottish Centre for Telehealth & Telecare

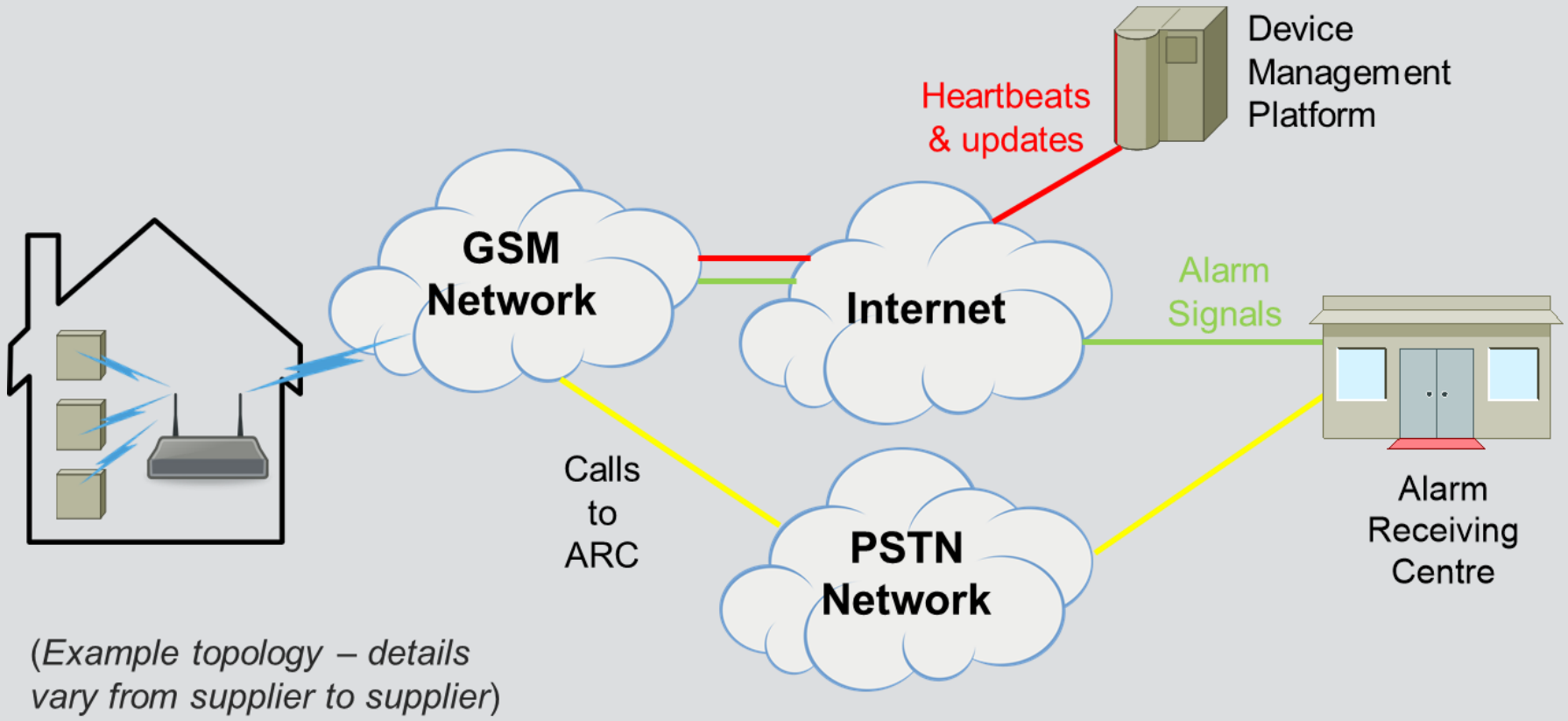
NHS 24

digitaloffice.scot

WHY DOES IT MATTER - ANALOGUE

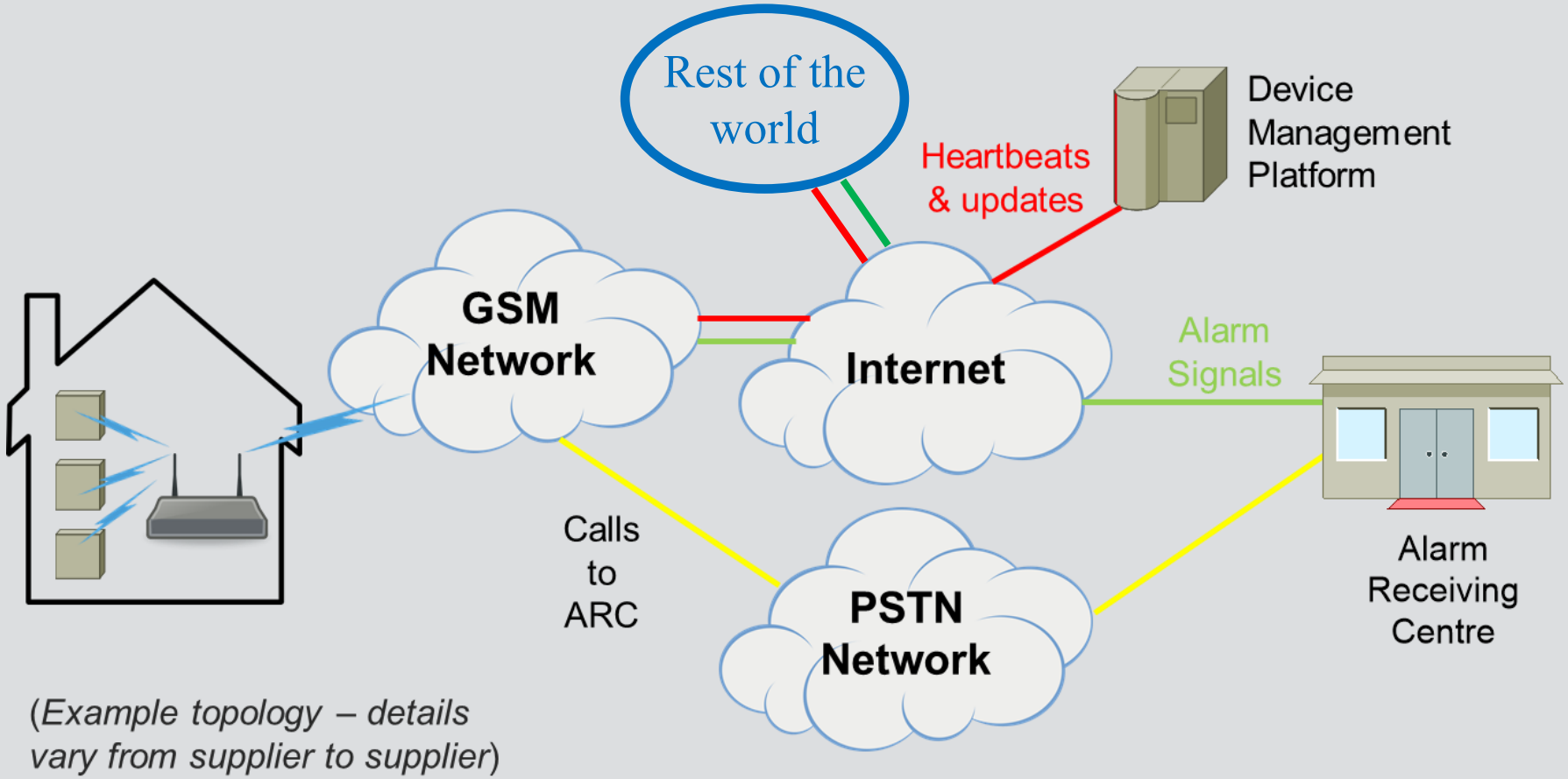


WHY DOES IT MATTER - DIGITAL



(*Example topology – details vary from supplier to supplier*)

WHY DOES IT MATTER - DIGITAL



(*Example topology – details vary from supplier to supplier*)

DIGITAL OFFICE
Scottish Local Government

TEC Technology Enabled Care

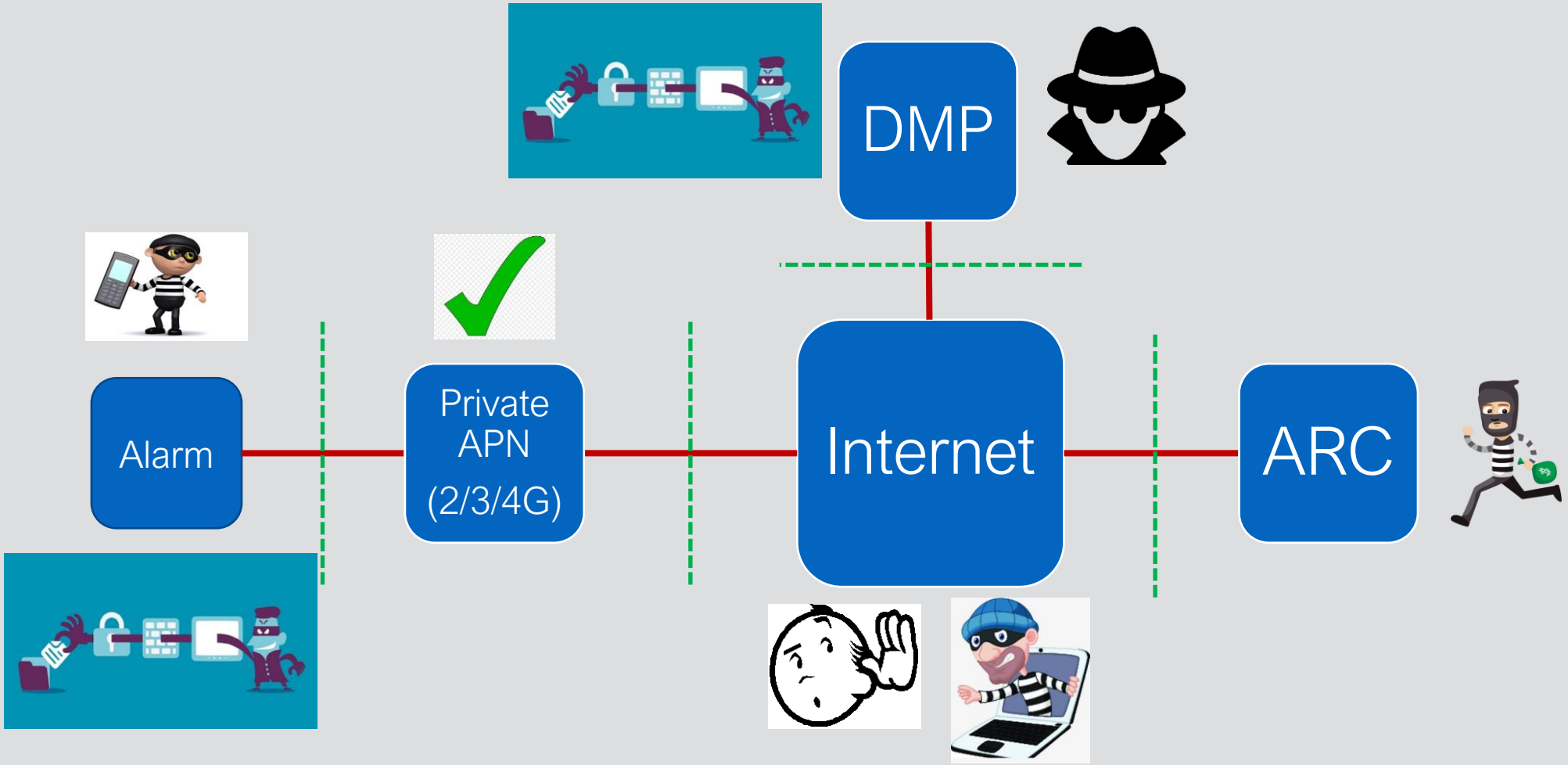
Scottish Centre for Telehealth & Telecare

NHS 24

WHY DOES IT MATTER – WORST CASE SCENARIOS

- A local criminal is able to steal a mobile SIM and run up a huge phone bill
- A bored teenager is able to disrupt alarm signals or calls
- An international criminal is able to disrupt alarm signals or calls and hold the care provider to ransom
- An international criminal is able to gain remote access to sensitive care data in the ARC and then sell it or use it for personal gain
- Not an exhaustive list!

WHERE DO THE THREATS LAY?



SOLUTION (ATTEMPT 1) – HSCP LED

- Develop supplier questionnaire
- Distribute to Health and Social Care Partnerships for individual issuance to suppliers
- Provide guidance to HSCPs about minimum security standards for procurement

SOLUTION (ATTEMPT 1) – HSCP LED

- Good points
  - Light weight
  - Hands off
  - Enables HSCPs to apply their own risk methodologies
- Bad Points
  - Suppliers were frustrated at having to deal with multiple security dialogues across Scotland
  - No single HSCP had enough sway to mandate change in a supplier's security posture
  - HSCPs didn't have the resources or knowledge to challenge questionnaire answers

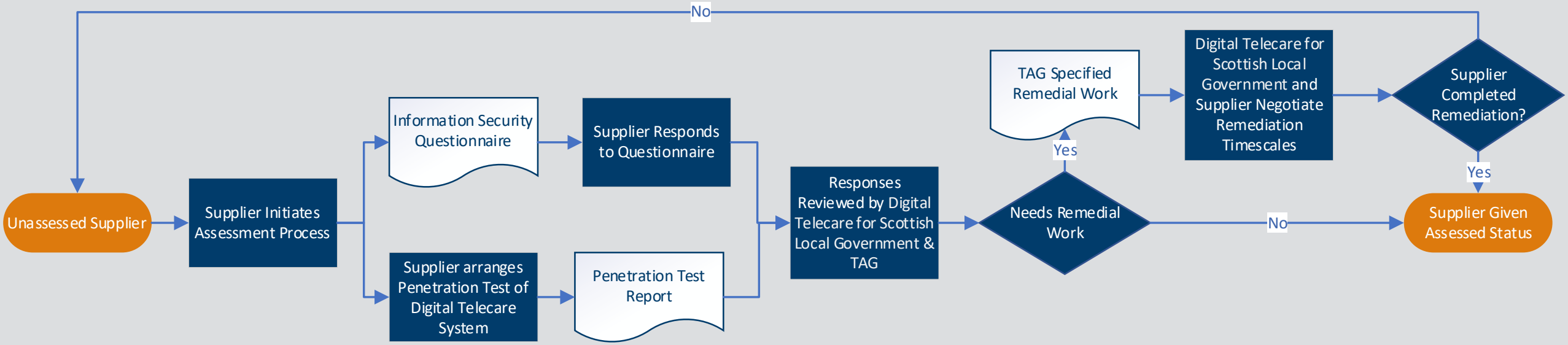
SOLUTION (ATTEMPT 2) – CENTRALISED ASSESSMENT PROCESS

- Key objectives
  - Voluntary
  - Maximum supplier engagement
  - Suppliers assisted in bringing their technologies up to the relevant standard
  - Trust between suppliers and assessors
    - **no commercial disadvantage for disclosing vulnerabilities**
  - Simple process for HSCP project managers with limited technical knowledge
  - Zero cost for HSCPs
  - Limited cost for suppliers

SOLUTION (ATTEMPT 2) – CENTRALISED ASSESSMENT PROCESS

- Refine supplier security questionnaire and issue to each supplier once
- Enter into NDA with each supplier
- Supplier pays for penetration testing of devices and services to be offered for sale in Scotland
- Risk based assessment of devices, services and supplier
- Supplier is then either:
  - Accepted onto assessed supplier list /or/
  - Accepted onto list with an agreed timetable for remediations /or/
  - Offered remedial guidance to improve and welcomed for reassessment
- Scotland Excel introduces a question relating to the supplier assessment scheme into their new digital telecare framework

ASSESSED SUPPLIER SCHEME OVERVIEW



DIGITAL OFFICE
Scottish Local Government

TEC Technology Enabled Care

Scottish Centre for Telehealth & Telecare

NHS 24

digitaloffice.scot

OUTCOMES

- High proportion of existing Scottish market have engaged with the scheme
  - and some new providers
- First supplier, device and service went live on the list end Jan 2021
- New devices and services being assessed weekly
- 21 vulnerabilities or issues detected so far
  - 6 remediated by suppliers immediately
  - 15 have an agreed timetable for rectification
- Suppliers have issued letters of intent to achieve industry recognised standards, where they do not already hold one (e.g. ISO 27001)
- Positive feedback from suppliers about the approach

Implementing a voluntary security assessment scheme for suppliers:

Our experiences and conclusions

Dr Andy Grayland
CISO
Digital Office – Scottish Local Government

DIGITAL OFFICE
Scottish Local Government

TEC Technology Enabled Care

Scottish Centre for Telehealth & Telecare

NHS 24

digitaloffice.scot