Security Areas of Focus

- **Security Governance**
  - Ability to manage end-to-end smart meter security on an ongoing basis.
  - Threat assessments.
  - Incident management.
  - Security audits/reviews.

- **Technical Security**
  - Standards for protection of Confidentiality, Integrity & Availability of data and systems.
  - Cryptography and principles for key management.
  - Use of existing industry standards.

Security Update

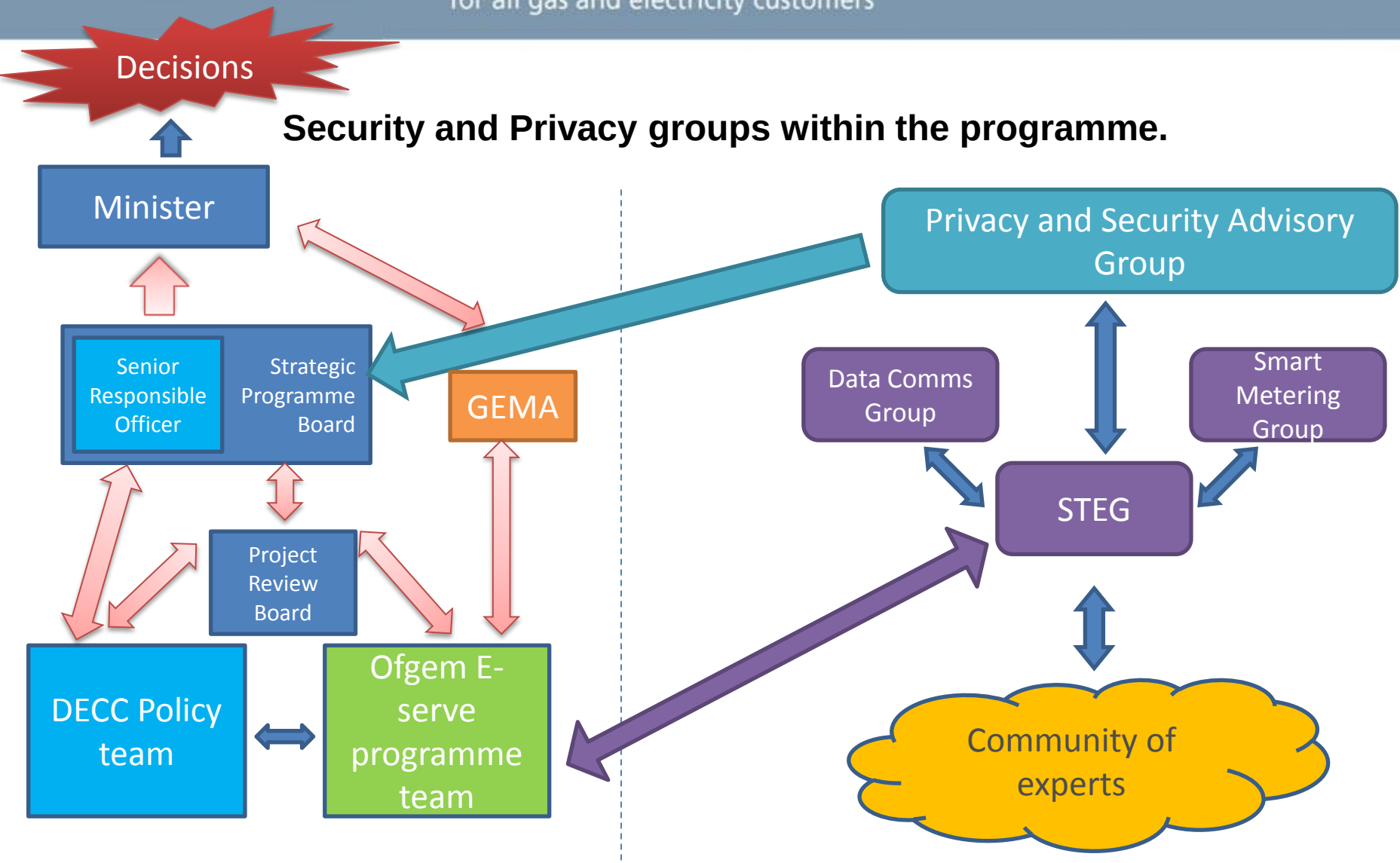
- **End-to-end Risk Assessment to drive security options and selection of countermeasures**
- **Proposals in areas of Security Governance and Technical Security**
- **Security proposals will be developed to inform design working group decisions**
- **Security Technical Expert Group (STEG) is platform for discussing security options**

Security Risk Assessment

- **IS1 tool – Government Methodology for Risk Assessments**
  - Define threats actors and threats.
  - Assign values for likelihood of threat (based on motivation/capability).
  - Determine impact of threats (operational / financial / reputational).
  - Prioritisation of risks.

- **Example Risks:**
  - Cyber threats via targeted malware or hacking attacks which could result in loss of meter functionality or remote connect/disconnect events.
  - Insider threats to the DCC and/or suppliers that leads to high profile information leakage and/or disruption to communication with smart meters.
  - End user threats from crime/fraud; i.e. customers attacking meters for financial gain.

Security and Privacy groups within the programme.



Privacy Update

Prospectus outlined our proposal that:

"The customer shall choose in which way consumption data shall be used and by whom, with the exception of data required to fulfil regulatory duties."

Working to Privacy by Design principles:

- Ensuring that data privacy is built into the smart metering system and services provided to facilitate this.
- Looking at the regulatory framework to allow smart metering data to meet current needs and respond to market throughout the projects lifespan.

Working with stakeholders:

- Understanding points raised in consultation responses
- Data use workshops – engaging critics
- The extension of an advisory group

Working with best Practice from the Information Commissioners office:

- Looking at the need for sector specific
- Carrying out a Privacy Impact assessment

Privacy Impact Assessment

What is a Privacy Impact Assessment?

- Undertaken early in project life-cycle
- In-depth review of proposed system infrastructure
- Assessment of compliance with relevant legislation and likely impact on privacy

Objectives:

- Identify, assess and mitigate data protection and privacy risks
- Ensure compliance with legal and regulatory requirements
- Facilitate a privacy-friendly approach to project design and implementation

Outputs:

- Full assessment report due in March
- Recommendations for any remedial action
- Feedback to Programme