Review of Indicative Table of Contents for the Smart Energy Code

Service Lines
DCG SG3
21 December 2010

Data privacy

The Prospectus says:

"…measures in relation to data privacy…[and].. ..deal with the circumstances under which consumers could authorise their own service providers, such as energy service companies, to access their data"

Data privacy principles

- **Assumption the output from the privacy Group will determine this section of the Code – definitions and standards**
- Info some key questions:
- Scope of governance & accountability – who owns & monitors data privacy in DCC & other organisations? How will this be defined?
- The DPA is fairly broad – should a specific Data Privacy Standard/Privacy Assessment be defined under ICO?
- Should the type and scope of data able to be used and processed by the relevant entities be defined? i.e. DCC, direct organisations, 3rd parties.
- Should all organisations and the DCC conduct Privacy Impact Assessments, or more detailed full Risk Assessments?
- Should there be independent auditing & verification of Data Security & Privacy controls?
- Consumer choice on data usage – how is this owned and managed?
- How should access to personal data be controlled?
- How should Privacy incidents and breaches be reported and managed?
- Needs to be proportionate for DCC and different parties.

Security & Business Continuity

The Prospectus says:

"…arrangements relating to the security of the communications network and for business continuity"

Data security principles

- **Assumption the output from the Security Group will determine this section of the Code – definitions and standards**
- Info some key questions:
- Scope of governance & accountability – who owns & monitors Data Security in DCC & other organisations? Should specific roles be mandated both globally and within each organisation?
- Technical as well as Data Security Management – should there be separate standards?
- Best practice standards – ISO27001, SPF, DPA1988, EU-DPD – is this sufficient? Should a specific information security standard be created for Smart systems or is ISO27001 / SPF enough?
- Should there be independent auditing & verification of Data Security & Privacy controls?
- Should formal risk assessment and risk management processes be required for all organisations? Should this be IS1 or ISO27001?
- Should ISO27001 certification be required for any or all entities?
- How should Security incidents and breaches be reported and managed?
- How should security incidents and suspected vulnerabilities be collated and fed back to the community to ensure countermeasures are implemented?
- Should a technical group be available to address any new vulnerabilities discovered?

Business continuity principles

- Scope of Business Continuity should be complimentary and proportionate – Who should have formal BC plans - DCC, other organisations? What systems / services / processes should be mandated, if any?
- Data recovery would be required – define process
- Should a standard such as BS25999 be used to provide independent accreditation?
- Should BC Plans be independently audited for suitability? By whom? e.g. DCC auditor
- BC plans – who approves them for suitability? Should a responsibility framework be defined? e.g. SEC Panel
- How should plans be tested? Should this testing be monitored and reported? e.g. SEC secretariat
- Should there be a common invocation /reporting procedure to notify other entities, DCC, Ofgem etc?
- Link with ISO27001 (as includes BC elements)
- Contractual arrangements should define BC requirements between DCC and data communications service providers

Performance management

The Prospectus says:

"…Performance levels, performance monitoring and incentivisation…..service levels in relation to communication and data services, how these services would be monitored and, in broad terms, the basis for incentivisation. Details of the incentivisation would be set out in contracts between DCC and its service providers."

Performance management principles

- Clarity of the service provided i.e. specified in service descriptions section?
- Whole service covered deliverables but some may have different service levels
- Definition of measurement (clear standards)
  - service availability - %
  - timeliness – delivery & response timelines
  - query management
  - maybe dependent on usage profiles, e.g. rules for users
  - others?
- Suspension rules
  - planned & unplanned (link with Force Majeure)
- Details within subsidiary documents

Performance monitoring

- Link to Reporting section 22 under DCC management – avoid duplication
- Proportionality – monitoring costs < user benefits
- Robust, verifiable service metrics – independent collation/check?
- Whole service may be covered with different levels for different services
- Frequency of reporting – daily, weekly, monthly, quarterly?
- Report to whom – Panel, all users, Ofgem?
- Consequences of failure (link to LDs, Liability, Default)

Incentivisation

- Assumption within licence as price controlled entity
- Negative or positive incentivisation or both
  - targeted LDs for poor service – (assumption within SEC)
  - Bonus payments for exceeding service levels – some reservations (assumption within licence)
  - Cap & collar approach? – (assumption if included in licence, defined in price control elements)
- LDs and bonus payments: reflective of loss or gain to users – clear definition of when paid & how much
- Flexible to be able to encompass development of service i.e. amended performance levels or new service lines
- DCC is liable but likely to be backed off with its service providers – is this a [licence] requirement?

N.B. DCG have developed papers on DCC incentivisation

Business processes

The Prospectus says:

"There would be a number of business processes under the Code that would need to be documented."

Business processes - scope

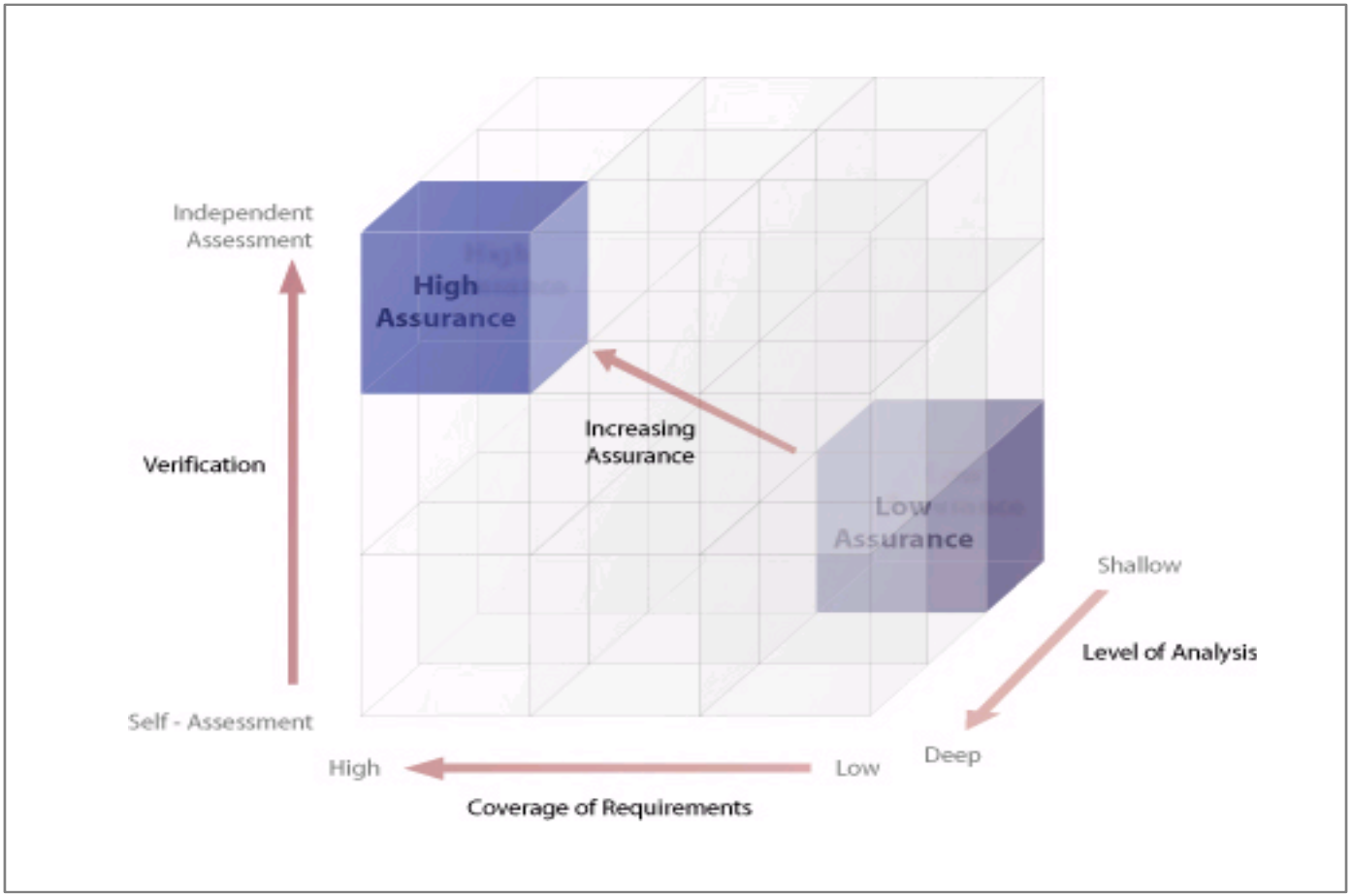
- Should business processes be part of main body of SEC or within supplementary documentation e.g. Agreed Procedures, Schedules?
  - View that principles in main body with detail in Code subsidiary documents – if so given force through Code's main provisions
- Potential duplication with other SEC sections e.g. modifications within Governance section
- What processes need to be defined & managed through the Code?
- Do we need E2E diagrams & golden threads? Yes in subsidiary documents but too early to develop yet – Phase 2.
- Subject to same modification process or simplified?
- Cross references to other agreed procedures, e.g. meter governance

Assurance

The Prospectus says:

"System and process assurance…..to include assurance provisions under the Code including the preparation of some form of risk identification and management plan"

Assurance principles



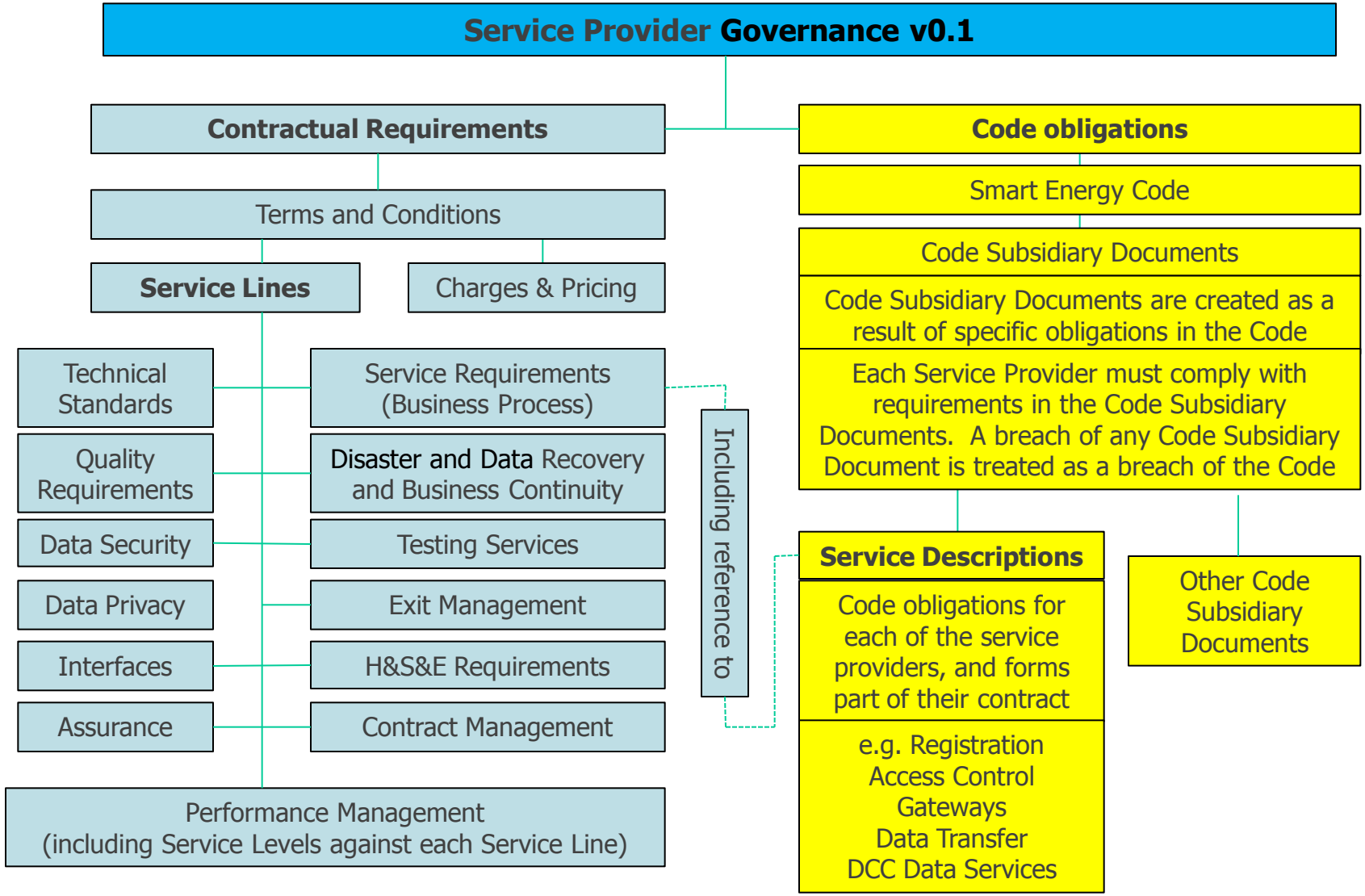
What level of assurance is required?

Scope of assurance

- System & process assurance – adopt risk based approach
  - which parties? DCC (& service providers) & SEC parties
  - integrated system or process testing?
  - Market readiness – implementation & new entrants (inter-participant testing)
  - Go live criteria – "Go/No Go": Ofgem/DECC decision – any elements in code?
  - Enduring operation including new services and/or modifications – requalification
  - Must be proportionate
- SMS assurance
  - Compliance with technical specifications – may reside in code but dependent upon SMDG outputs
- Who undertakes & reports to whom?
  - Fully independent assurance or verifies testing results? Different assurance providers for different service lines?
  - SEC Panel. Users, Ofgem?
  - Remedies if fail assurance regime
- Interaction with assurance regimes within existing codes – avoid duplication

Scope of assurance

- Assumption – potential for techniques within code and the detail within subsidiary documents.
- What procedures/processes are subject to assurance? Adopt risk based methodology?
- Detailed assurance procedures – in main body or subsidiary documents?
- Risk identification & management plan
  - duty for SEC Panel to identify risk and manage it, e.g. assurance and performance monitoring?
  - should DCC be required to provide these i.e. a service line or via commercial arrangements?


Service Provider Governance v0.1
Contractual Requirements
Terms and Conditions
Service Lines
Charges & Pricing
Technical Standards
Quality Requirements
Data Security
Data Privacy
Interfaces
Assurance
Service Requirements (Business Process)
Disaster and Data Recovery and Business Continuity
Testing Services
Exit Management
H&S&E Requirements
Contract Management
Performance Management (including Service Levels against each Service Line)
Including reference to
Code obligations
Smart Energy Code
Code Subsidiary Documents
Code Subsidiary Documents are created as a result of specific obligations in the Code
Each Service Provider must comply with requirements in the Code Subsidiary Documents. A breach of any Code Subsidiary Document is treated as a breach of the Code
Service Descriptions
Code obligations for each of the service providers, and forms part of their contract
e.g. Registration
Access Control
Gateways
Data Transfer
DCC Data Services
Other Code Subsidiary Documents

Service Lines – content v0.1