Risk Management Strategy

Version:	**V4.0**
Date:	**2 April 2020**
Classification:	**DCC Public**

Document Control

Revision History

Revision Date	Summary of Changes	Version Number
19 Dec 2013	Original Document	2.0
Oct 2016	Document updated to reflect changes in DCC operating model and organisation structure	3.0
1 August 2019	Document updated to reflect changes in DCC operating model and organisation structure including the establishment of an Internal Audit function	4.0

Document Approval

Name	Title / Responsibility	Date
Jacqui Russell	Head of Metering and Market Operations, Ofgem	2 April 2020
Angus Flett	Chief Executive Officer, DCC on behalf of DCC Board	2 April 2020

Table of Contents

1 Context

The Smart Data Communications Company Ltd (DCC) was awarded the Smart Meter Communication Licence (the Licence) in September 2013. The Licence defines the conditions under which the DCC will implement and manage a data and communications service that enables smart meters installed within UK domestic and non-domestic premises to communicate with the business systems of authorised DCC Service Users.

Condition 6 of the Licence defines the Authorised Business activities that the DCC is permitted to deliver.

Condition 7 of the Licence sets out the requirement for DCC to operate general controls for the Authorised Business. The requirements of Licence Condition 7.13 are summarised below:

Part A: Corporate Governance. The DCC must comply with the principles of the UK Corporate Governance Code as if it were a quoted company.

Part B: Internal Controls. The DCC must define and operate systems and procedures for internal control of activities comprising the Authorised Business.

Part C: Risk Management. The DCC must operate a Risk Management Strategy providing a robust framework for the identification, evaluation and management of risk with respect to the Authorised Business. The DCC Risk Management Strategy must, in particular:

a) explain the Licensee's attitude to, capacity for, and tolerance of Authorised Business Risk;
b) enable Authorised Business Risk to be identified across all the Authorised Business Activities along with an assessment of the materiality in each case;
c) require the maintenance of a permanent register of Authorised Business Risk;
d) require the maintenance of a plan for the purpose of recovering or continuing Authorised Business Activities after any natural or human-induced disaster;
e) contain evaluation criteria in respect of Authorised Business Risk that are to be reviewed annually; and
f) provide for the allocation of resources in respect of Authorised Business Risk.

This document describes the DCC Risk Management Strategy, as required by part C.

2 Risk Appetite

Financial Reporting Council guidelines for UK Corporate Governance state that when determining principal risks, the Board should focus on risks that could threaten the company's viability and sustainability, including threats to:

- Business model,
- Future performance and ability to deliver strategy,
- Solvency and liquidity

This is interpreted for the DCC as follows:

Risk type	DCC Interpretation
Business model	Threat to the DCC retaining the Licence due to a revocation event or service failure, or reputational damage putting future Licence renewal at risk
Future performance and ability to deliver strategy	Threat to the DCC delivering expected business performance
Solvency and liquidity	Threat to solvency or liquidity of the Company

The DCC risk appetite for the Authorised Business is outlined below:

Risk type	Context	Risk appetite
Threat to the DCC retaining the Licence due to a revocation event or service failure, or reputational damage putting future Licence renewal at risk	A security breach or data loss incident could have significant consequences for our customers and energy consumers and is a significant threat to the business. In addition, the company faces significant operational and delivery challenges in support of the SMIP and other associated industry programme objectives. Failure to deliver against these requirements puts the future extension of the Licence at risk.	Security is a primary focus for the Board. The DCC will have a low appetite for risks that threaten security or data protection. The DCC will have a medium appetite for risk that could threaten delivery of SMIP or other industry programme outcomes, reflecting the scale, complexity and uncertainties inherent in DCC program delivery.
Threat to the DCC delivering expected business performance	Key risks include: • Failure to ensure that the Smart Metering Implementation Programme is delivered within the cost profile approved in the annual Charging Statement • Failure to deliver to Operational Performance Regime (OPR) targets • Disallowance of costs as a result of Price Control decisions by Ofgem • Failure to deliver our Business Plan targets for innovation or re-use of the smart metering network	The DCC will have a low appetite for risks that threaten business performance.
Threat to solvency or liquidity of the DCC	Key risks include: • Failure to properly manage our cash position • A material financial fraud	The DCC will have a low appetite for risks that threaten Company solvency or liquidity.

3 Risk Management Approach and Governance

The DCC operates a risk management approach consistent with the UK Corporate Governance Code and the principles of BS ISO 31000:2018. An overview of the DCC risk management framework is shown in figure 1 below:

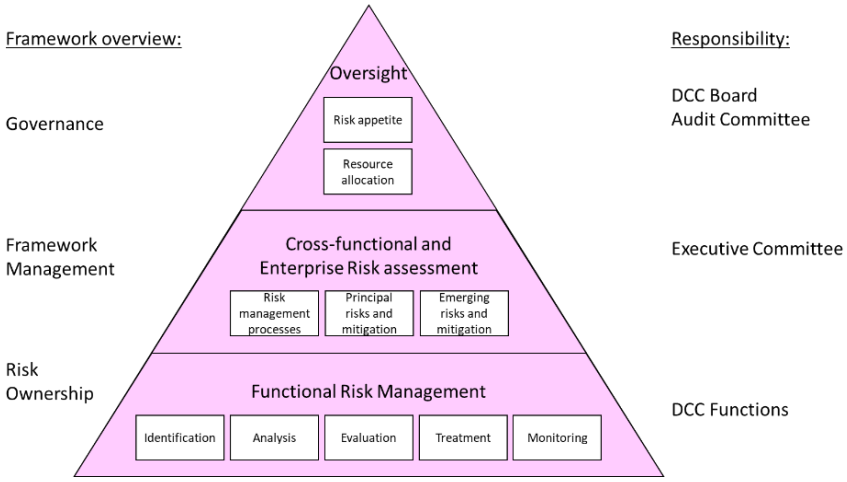

Figure 1: risk management framework

The DCC Board is responsible to approve the DCC risk management systems and framework, to set the DCC risk appetite, and to ensure that the necessary resources are in place to manage risk effectively. The DCC Audit and Risk Committee (ARC) is responsible to monitor the effective operation of the risk management systems and framework.

The DCC Executive Committee (ExCo) is responsible to lead the implementation and operation of the risk management systems and framework within the DCC, and to develop the Enterprise Risk assessment representing the principal risks affecting the Authorised Business of the DCC. ExCo are responsible to monitor the risk environment on an ongoing basis, including both principal risks and new and emerging risks, and to ensure that the Enterprise Risk assessment reflects the best available information.

Enterprise Risks are reviewed regularly by the ARC. Recommendations on risk tolerance, remediation actions, and resource allocation are made by the ARC and approved by the DCC Board.

DCC functions are responsible for day-to-day management of risk, and risk awareness and risk management are an inherent responsibility of all DCC staff. Each DCC function is responsible to identify, manage and report risk according to a standard risk assessment framework and to maintain a functional risk register detailing identified risks, mitigation actions and owners. Risk management and reporting is also embedded into key business processes, including:

- Business plan development and reporting
- Programme delivery governance and reporting
- Operational performance governance and reporting
- Financial performance governance and reporting
- Contract development and approvals including contract change
- Service Provider performance management and reporting
- Internal Audit and Compliance reporting

Operation of the DCC risk management framework and processes is audited and assured by the Business Improvement and Audit function and reported to the ARC.

The risk review and reporting structure is summarised below:

Governance Level	Responsibility
DCC ExCo	• Ongoing operation and compliance with key risk management processes • Monthly review of key functional risks, including programme delivery and operational risks • Monthly review of Enterprise Risk mitigation action status and completion • Quarterly review of Enterprise Risk assessment and action plan, including any new or emerging risks • Annual Enterprise Risk refresh
DCC Audit Committee	• Regular review of the Enterprise Risk assessment and action plan, including resource allocation, for recommendation to DCC Board • Annual review of the risk management systems and framework
DCC Board	• Monthly review of DCC key program delivery risks and mitigation plans • Approval of Enterprise Risk assessment and mitigation plan as recommended by ARC • Approval of DCC risk management system and framework as recommended by ARC

Given the nature of the Authorised Business and the DCC's special position according to the Licence, the DCC also actively engages with the Department for Business, Energy and Industrial Strategy (BEIS), the Licence Authority (Ofgem), and DCC customers in order to effectively manage overall industry and programme risks.

The stakeholder engagement approach is summarised below:

Stakeholder group	Risk Management Approach
DCC and Service Providers	• Internal governance and risk management
BEIS and Ofgem	• Bilateral governance and/or other mandated forums as appropriate
DCC Customers	• SEC Panel and/or other subsidiary or associated industry forums as appropriate

4 Risk Assessment Framework

DCC has adopted a standard framework and definitions for risk assessment across the business. Definition of the key terms is summarised below:

- Risk likelihood: the probability that the risk will materialise
- Risk Impact: the consequence for business operations should the risk materialise
- Risk Assessment: the overall risk rating, taking likelihood and impact into consideration
- Inherent risk: worst-case risk assessment before any mitigating controls are considered
- Residual risk: risk assessment after existing, in-place mitigating controls are considered
- Risk Appetite: proposed acceptable risk tolerance, which may require further mitigating action

Risk Impact categories are defined as follows:

Risk Impact	Description
Severe	An impact which will cause the organisation to lose the capability to operate, or an incident that interrupts the business sufficiently to threaten its viability
Significant	Widespread, abnormal situation which threatens the business, linked to a period of time when the business is not able to operate as expected
Moderate	An event which interrupts normal business functions leading to a failure to fulfil agreed requirements or expectations
Minor	A brief, localised concern, affecting a specific set of circumstances

The risk assessment matrix is outlined in figure 2 below:

	Likelihood rating:			
Impact rating:	Remote or Rare (10-20%)	Possible or Marginally Likely (20-50%)	Frequent or Probable (50-75%)	Imminent or Certain (75-100%)
Severe	**HIGH**	**CRITICAL**	**CRITICAL**	**CRITICAL**
Significant	**MEDIUM**	**HIGH**	**HIGH**	**CRITICAL**
Moderate	**LOW**	**MEDIUM**	**HIGH**	**HIGH**
Minor	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**

Figure 2: risk assessment matrix

5 Business Continuity and Disaster Recovery

The DCC maintains a comprehensive Business Resilience framework and Business Continuity and Disaster Recovery (BCDR) plans, consistent with the requirements of the Smart Energy Code (SEC) Section H10.

The scope of the DCC Business Resilience framework is outlined in figure 3 below:

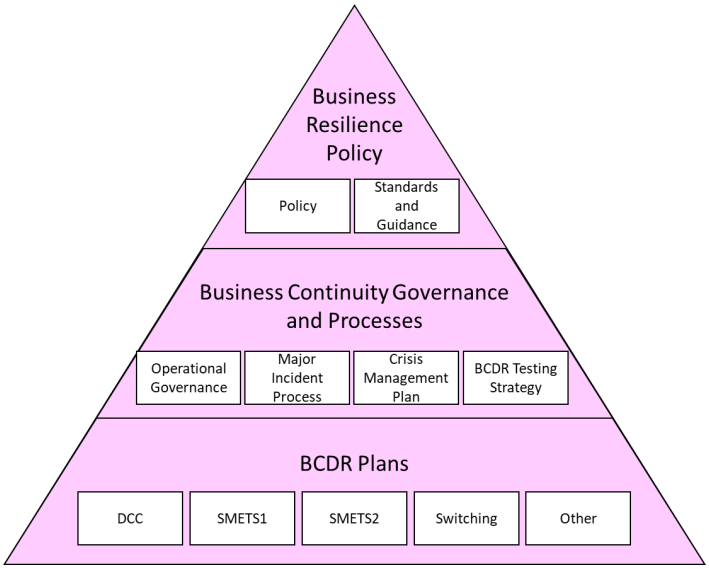

Figure 3: Business Resilience framework

The Business Resilience Policy defines the DCC approach to Business Continuity Management (BCM). The DCC BCM approach is a holistic management process to identify potential threats and their associated impact to business operations and provide a framework for managing an effective response that safeguards the interests of DCC's key stakeholders including DCC Users.

The Business Resilience Policy applies to both the DCC as Licencee and to all DCC Service Providers that provide services in support of the Authorised Business, including existing SMETS2 services, existing and in-development SMETS1 services, in-development switching services, and other potential future services. All relevant Service Providers are required to produce and maintain a BCDR plan, which is integrated into the overall DCC BCDR plan at the point of operational acceptance into live service.

The purpose of each component of the Business Continuity Governance and Process framework is described below:

Component	Purpose
Operational Governance	• Maintain the Business Resilience Policy and ensure policy compliance • Review and assess changes to BCDR risks, context and requirements • Maintain and assure DCC and Service Provider BCDR plans, and to ensure coherence and consistency between BCDR processes
Major Incident Process	• Ensure effective collaboration, coordination and standard working practices between DCC and Service Providers to restore service as quickly as possible
Crisis Management Plan	• Ensure a consistent and controlled approach between DCC, Service Providers and key stakeholders in response to a crisis event

BCDR Testing Strategy	• Ensure all appropriate activities and services are included in scope for BCDR testing • Ensure appropriate BCDR testing requirements are included in the design and delivery for new services

All Service Provider BCDR plans must comply with the relevant standards (BS ISO 27031 and ISO 22301) and are assured by the DCC. All BCDR plans are tested annually by DCC, as required by the SEC and in consultation with our customers.

Business Continuity testing exercises the business continuity plans for key operational services including Service Provider Service Operations Centres and Network Operations Centres, and DCC Service Desk. Testing includes the transfer and return of service from primary to secondary business location.

Disaster Recovery (DR) testing of IT infrastructure, network and operational services follows a standard process including:

- Review and testing of recovery performance against the approved DR 'Run Book'
- Testing of failover and failback performance against the specified Recovery Time Objective
- Proving of capability to operate services from the specified secondary site
- Testing of DR communications channels and processes and effective coordination

The outcomes of BCDR testing are reported to the SEC Panel.