

Risk Management Strategy



Version: V4.1
Date: 25 May 2021
Classification: DCC Public

Document Control Heading

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
25 May 2021	Document updated to reflect changes to DCC Risk Appetite Methodology and Board Review	4.1

Document Approval

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

Table of Contents

1	Context.....	4
2	Risk Appetite	5
3	Risk Management Approach and Governance	7
4	Risk Assessment Framework.....	8
5	Business Continuity and Disaster Recovery	10

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	<ul style="list-style-type: none"> • Threat to the DCC retaining the Licence due to a revocation event or service failure • Reputational damage putting future Licence renewal at risk
Future performance and ability to deliver strategy	<ul style="list-style-type: none"> • Threat to the DCC delivering expected core business performance • Failure to deliver future re-use and innovation strategy
Solvency and liquidity	<ul style="list-style-type: none"> • Threat to solvency or liquidity of the Company

DCC has adopted a risk appetite scale based on best practice as defined in the UK Corporate Governance Code and Government finance guidance¹. The scale is defined to support a balanced evaluation of both risk and reward, and to cover both financial and non-financial risks.

Risk Appetite	Definition	Reward vs risk ratio
Hungry	Willing to accept significant residual risk to achieve maximum return	Potential reward is significantly greater than risk
Open	Eager to be innovative and choose options offering potentially higher business rewards, despite greater inherent risk	Potential reward is greater than risk
Cautious	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing acceptable reward and value-for-money	Potential reward and risk are balanced
Averse	Avoidance of risk and uncertainty is a key organisational objective Preference for safe delivery options that have a low or very low degree of residual risk	Potential reward is lower than risk

¹ Risk Appetite guidance, UK Government Finance Function 2020, and Government Orange Book risk appetite framework 2020

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

Risk Type	Context	Risk Appetite
Licence Compliance	<p>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.</p> <p>A persistent non-compliance with Licence or Codes, a revocation event, or a material consumer-impacting service failure could put Licence retention at risk.</p>	Averse
Reputation	<p>DCC reputation reflects stakeholder confidence in delivery, service performance, value-for-money, and cost management.</p> <p>Positive DCC reputation reflects confidence for continued operation of the core network and services and opportunity for re-use and innovation.</p> <p>Poor reputation increases the likelihood of regulatory intervention and puts future extension of the Licence at risk.</p>	Cautious
Core Business Performance	<p>DCC prioritises delivery of core business services and performance. Core business performance risks include:</p> <ul style="list-style-type: none"> • Inadequate internal or system-wide processes and controls • Service Provider performance failure • Lack of DCC capability, skills, or knowledge • Failure to effectively manage stakeholder requirements <p>The consequences of failure to deliver expected core business performance include:</p> <ul style="list-style-type: none"> • Failure to deliver within the cost profile approved in the annual Charging Statement • Failure to meet Operational Performance Regime (OPR) targets • Disallowance of costs as a result of Price Control decisions by Ofgem • Failure to deliver DCC Business Plan targets 	Cautious
Re-use and innovation	<p>DCC strategy is to maximise public good benefits from the smart metering infrastructure through re-use of the network and capabilities and enabling innovation in new services, within the scope of activity approved by key stakeholders including BEIS and Ofgem.</p> <p>Successful delivery of the DCC strategy will maximise benefits and return to consumers, DCC customers and stakeholders.</p> <p>Key risks include:</p> <ul style="list-style-type: none"> • Failure to identify and pursue value-maximising opportunities • Failure to enable innovation at the pace and scale that innovators require • Failure to secure stakeholder support 	Hungry
Solvency and liquidity	<p>DCC must manage solvency and liquidity to ensure business viability and to retain shareholder and stakeholder confidence in prudent financial control. Key risks include:</p> <ul style="list-style-type: none"> • Failure to properly manage DCC cash position • A material financial fraud 	Averse

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:

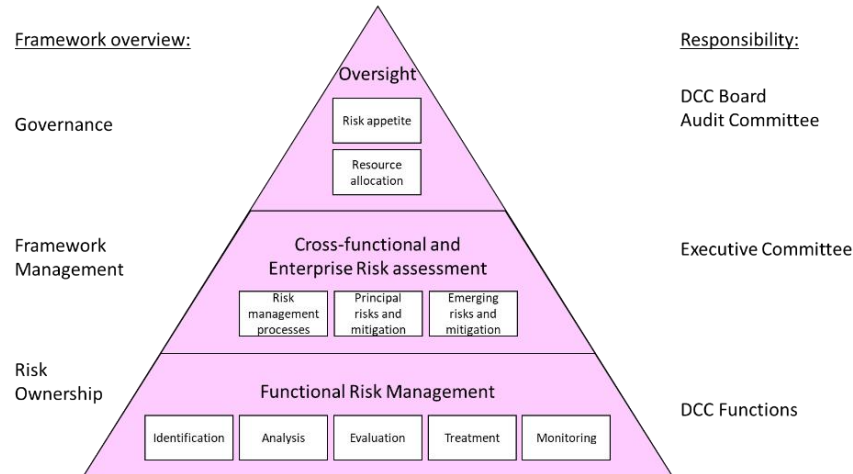


Figure 1: risk management framework

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	<ul style="list-style-type: none"> • Ongoing operation and compliance with key risk management processes • Monthly review of key functional risks, including programme delivery and operational risks • Quarterly review of Enterprise Risk assessment and mitigation action plans, including any new or emerging risks • Annual Enterprise Risk refresh
DCC Audit Committee	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 • Annual review and approval of Enterprise Risk assessment and risk appetite

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	<ul style="list-style-type: none"> • Internal governance and risk management
BEIS and Ofgem	<ul style="list-style-type: none"> • Bilateral governance and/or other mandated forums as appropriate
DCC Customers	<ul style="list-style-type: none"> • 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

Risk impact and likelihood are combined to establish an overall risk rating according to the risk assessment matrix outlined in figure 2 below:

	Likelihood rating:			
	Remote or Rare (10-20%)	Possible or Marginally Likely (20-50%)	Frequent or Probable (50-75%)	Imminent or Certain (75-100%)
Impact rating:				
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:

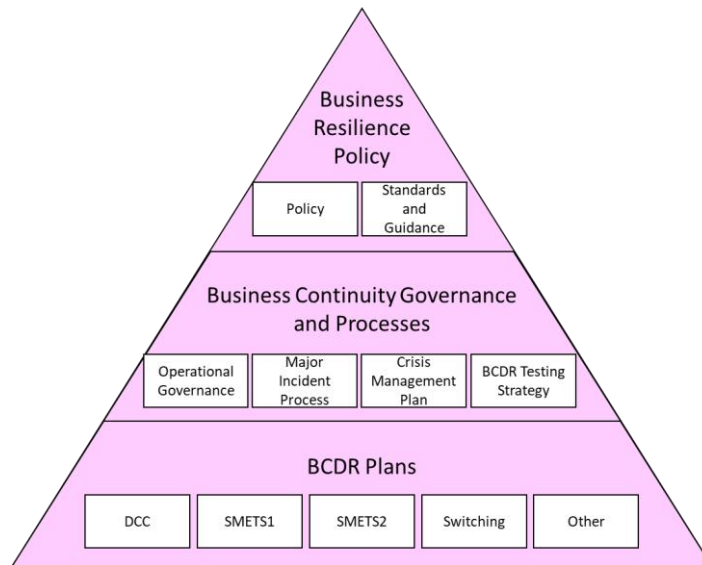


Figure 3: Business Resilience framework

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Ensure effective collaboration, coordination and standard working practices between DCC and Service Providers to restore service as quickly as possible
Crisis Management Plan	<ul style="list-style-type: none"> • 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.