Data Communications Company

Smart DCC
Risk Management Strategy

Version: 4.2
Date: March 2025

Revision History

Revision Date	Summary of Changes	Version Number
19 Dec 2013	Original Document	2.0
1 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
11 March 2025	Document updated to reflect changes to DCC Risk Appetite and Board Review of DCC's Principal Risks. Update to reflect the annual review of Register and Appetite	4.2

Document Approval

Name	Title / Responsibility	Date
Ayena Gupta	Head of DCC Oversight and Regulatory Review, Ofgem	22 July 2025
Gavin Robertson	Chief Finance Officer, DCC on behalf of DCC Board	11 March 2025

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 appropriate organisational structures, systems and procedures which are transparent and effectively monitored 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:

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.
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. Principal Risks and Risk Appetite

The Financial Reporting Council guidelines for UK Corporate Governance state that when determining principal risks, and Appetite for Risk, 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

For DCC we interpret this broad overview of threat as follows:

Risk Type	DCC Interpretation
Business model	That the business model, as defined by the Licence, can support the achievement of the core purpose of digitisation of energy use and the successful delivery of core obligations of **Reach** (ensuring all eligible premises can have a smart meter), **Security** (operate to CNI standards), and **Public Good** (maintain a platform to enable public policy implementation for consumer benefit).
Future performance and ability to deliver strategy	That the Company can fully implement its Strategy to maintain and enhance the Core Operating Platform performance and deliver mandated services while also expanding access to new customers, new capabilities and new services.
Solvency and liquidity	That the Company can maintain its solvency and liquidity, while delivering **value for money** and the lowest unit cost and that the solvency and liquidity of our core supply chain which delivers mandated services is maintained.

In delivering its Risk Management Strategy, the DCC uses a 3-point scale and terminology to define Risk Appetite which evaluates both risk and reward as outlined below:

RA Scale	Risk Appetite definition	Reward vs risk
Open (High)	•Eager to be innovative and choose options offering potentially higher business rewards, despite greater inherent risk	Reward > risk
Cautious (Medium)	•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 VfM	Reward ≈ risk
Averse (Low)	•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	Reward < risk

Risk Appetite is defined and set by the Board, is reviewed annually to ensure it reflects our core obligations.

Therefore, DCC have structured its Principal Risk appetite for the Authorised Business as follows:

Risk type	Context	Risk Appetite
• **Business Model**	The Smart Meter Licence has been extended to 2027 as DESNZ, and the Regulator finalise and agree the future Regulatory framework in which DCC shall operate and DCC's long term ownership. During the extension period DCC will work with all stakeholders and the Regulator to ensure that Licence renewal changes and timescales can be met while maintaining obligations.	DCC will take a **Cautious** approach to risks which could impact the business's ability to operate to its existing mandate as well as implement the required transition.
	DCC are obligated to operate to the highest security standards as defined by **Critical National Infrastructure** (CNI), 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.	Security is a primary focus for the Board. The DCC are **Averse** to risks that threaten security or data protection.
• **Future performance and ability to deliver strategy.**	DCC is obligated to operate within a Regulated Governance Model, as defined within our Licence and Codes (e.g. HM Treasury Green Book process where applicable) which can result in extended Cycle Times, specifically the time to ensure alignment and agreement across all stakeholders via the Business case process. As we transition to a new regulatory pricing framework, DCC will work closely with Stakeholders and the Regulator to ensure business plans and cost forecasts support efficient maintenance and upgrade of mandated services.	DCC is generally **Averse** to risks which could impact our ability to maintain and develop our mandated services to the time, cost and quality expectations of our customers and wider stakeholders DCC is **Averse** to Risk which could result in a material negative financial impact to its shareholder.
	DCC operates a complex technology architecture which is inherent to the successful delivery of our strategy and our core obligations. Due to that complexity DCC are currently required to manage and upgrade End-of-Life technology and inherited technology limitations while continuing to deliver to customer expectations of service and cost. This architecture will take time to replace which must be achieved while maintaining continuity of service.	

Risk type	Context	Risk Appetite
• **Solvency & Liquidity**	DCC delivers against a wide range of obligations including societal benefits and public good through extension and re-use of DCC capability and services. DCC is expected to deliver Value for Money and its services in a sustainable way. DCC will ensure that it balances resource (time, people, and cost) to assure delivery of all our obligations, and will also ensure that all processes under its control will operate in an efficient way which provides value for money.	DCC is **Averse** to any Value for Money Risk for which we have direct control DCC will take a **Cautious** approach to Value for money Risk which is not fully in its control. which could impact on its ability to effectively balance resource across all its obligations

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 governance framework is shown in figure 1 below:

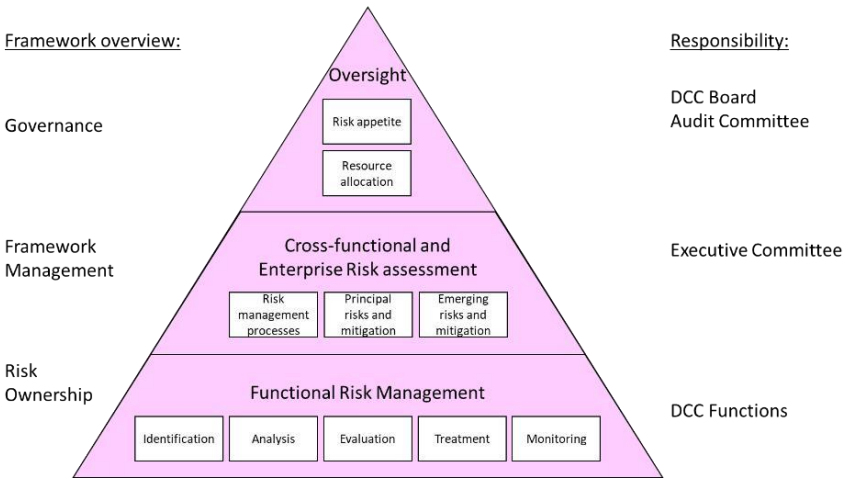


Figure 1: risk management governance framework

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.

Strategic 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.

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 Strategic and Operational 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 Strategic Risk assessment reflects the best available information.

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

Risk Hierarchy and structure:

To ensure that Risk is effectively owned, consolidated and managed across the business, and to ensure that emerging risks is appropriately escalated where necessary, DCC operates a top down-bottom up hierarchy and structures Risk ownership across 3 levels, as shown below.

DCC operates a top-down, bottom-up risk hierarchy. This means that Operational Risk feeds aggregated Business Risks that in turn aggregate into Strategic Risk.

Risk Type	Description	Accountable	Responsible
Strategic Risks	Smart DCC Board-set and Exco-owned risks that require enhanced oversight and focus. Strategic risks are often risk themes, made up of Operational risks identified by the organisation. These risks are set once per year and formally approved at the ARC. Risk mitigation responsibility sits with Exco for Strategic Risks.	Exco members	SLT members, Risk Mitigation Owners, 1st Line Risk Leads
Business Risks	Broad themes (listed in the DCC Risk Taxonomy) of aggregated Operational Risks. Business Risks help provide the linkage between Operational and Strategic level risks, enabling clear line of sight and enhanced reporting/visibility across the DCC risk landscape. Business Risks can either relate significantly to a Strategic Risk or can be an aggregation of Operational Risks where themes emerge that are not individually very impactful but collectively reflect a larger pattern of risk to the organisation.	Director Level and above	2nd Line Risk Management Team for maintaining the Risk Taxonomy. 1st Line Risk Leads, Mitigation Owners
Operational Risks	Operational Risks can relate to specific or multiple business areas and processes. Operational Risks are logged on business area risk registers on Risk Cloud which are maintained by the Risk Leads. Note – Some Operational Risks directly relate/support/roll up under one or more Strategic Risks.	Business Unit Leaders	1st Line Risk Leads and Mitigation Owners

DCC functions are responsible for day-to-day management of operational 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
- Price Control framework
- Contract development and approvals including contract change.
- Service Provider performance management and reporting
- Internal Audit and Compliance reporting
- Management across Product / Service Families and the operating Lifecycle of each Product Family

Operation of the DCC risk management framework and processes is audited and assured by the Risk and Assurance function and reported to the 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 DESNZ, the Licence Authority (Ofgem), and DCC suppliers and customers in order to effectively manage overall industry and programme risks.

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 crystalise.
- **Risk Impact**: the consequence for business operations should the risk crystalise.
- **Risk Assessment**: the overall risk rating, taking likelihood and impact into consideration.
- **Inherent risk**: worst-case risk assessment before any mitigating controls have been 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:

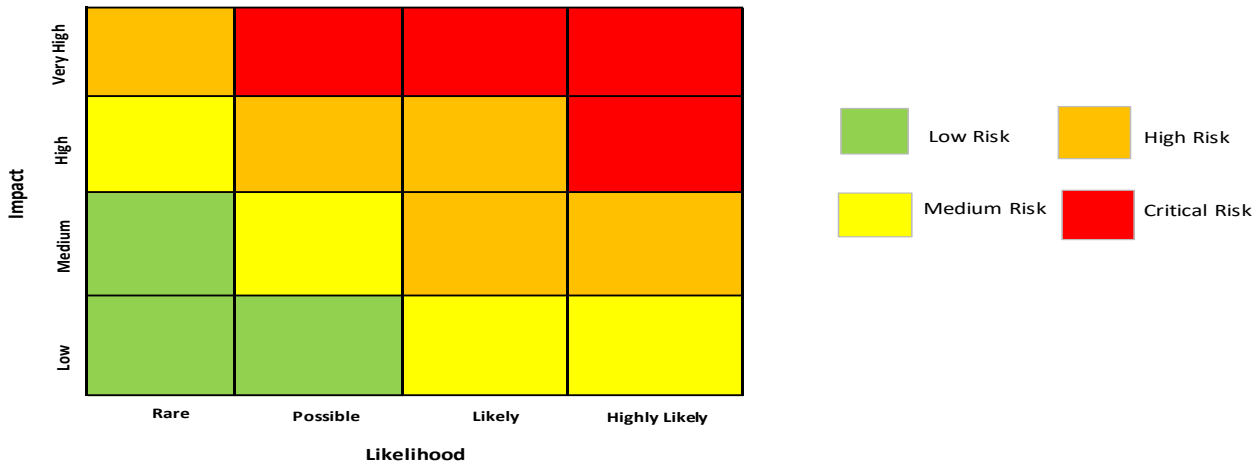
	Legal & Regulatory	Operational	Financial	Reputational
Very High (4)	Persistent failure to comply with licence principles leading to permanent licence revocation. Breaches in the law, especially relating to data protection and commercial practices.	An event with extreme loss of service, affecting >50% of our operations, services, customers or workforce	> Material cost increase vs ABP / Material Price Disallowance .	Irreparable negative coverage in tier 1 press and/or widespread social media. Lasting and significant damage to the DCC reputation with no ability to recover.
High (3)	Reportable breach or systemic breaches leading to increased regulatory scrutiny, formal and/or high-profile enforcement action and significant fines.	An event with a high loss of service affecting 25%-50% of our operations, services, customers or workforce	> Signiant cost increase vs ABP / Significant Price Disallowance	Multi-year reputational damage through negative tier 1 press coverage and/or significant social media reach. Resulting in a severe loss of trust with our stakeholders and/or the general public.
Medium (2)	Failure to comply with licence provisions and/or data protection laws leading to potential regulator enforcement and/or moderate fines.	An event with a medium loss of service affecting 5%-24% of our operations, services, customers or workforce	> Moderate cost increase vs ABP / Moderate Price Disallowance	Mostly negative national press coverage and/or social media traffic resulting in harmful reputational damage for up to one year.
Low (1)	Failure to comply with SEC or REC clauses or less significant licence provisions. Not leading to formal regulator action by itself, but a contributory factor in the event of multiple similar infringements.	An event with a low loss of service affecting <5% of our operations, services, customers or workforce	> Insignificant cost increase vs ABP / Insignificant Price Disallowance	Negative local and/or low-level social media coverage resulting in short term limited reputational harm.

Note that DCC maintains a detailed set of Risk Impact guidelines to support the table above which is available for all Risk owners.

Risk Likelihood is expressed as follows:

Rare <5%	Possible 5%-20%	Likely 21%-75%	Highly Likely >75%
Expected to only occur in exceptional circumstances	This could occur, but not likely	Probable. A reasonable chance that this will occur	Expected to occur in most circumstances

This translates to a **Risk Assessment Matrix** is outlined in figure 2 below:



Risk management Controls are regularly tested and reviewed against a defined scoring mechanism, which inform the rating of each Risk.

Control Implementation	
No Implementation	Controls Identified are not being followed
Limited	Controls Identified are not being followed regularly / completely, or other measures are being taken other than those identified
Partial	Controls identified are being followed but do not recorded / documented
Good	Controls identified are being followed, recorded and documented
Robust	Controls are well implemented regularly being reviewed and improved

Control Effectiveness	
No Control	Controls not in place
Limited	Little to no action being taken or planned. No protection systems exist or they have not been reviewed for sometime. No procedures are formalised and there is no review programme.
Partial	Some action being taken to control risks. Controls and systems are considered sub-standard and require improvement. It is likely that controls will fail to deal with the risk, if it occurs.
Good	Being addressed reasonably. Protection systems in place. Procedures exist for given circumstances. High level of confidence that controls will prevent risk from occurring or mitigate its consequence, if it occurs.
Robust	Viable controls are systematically implemented and reviewed.

5. Business Continuity and Disaster Recovery

The DCC maintains a comprehensive Business Resilience framework and Business Continuity and Disaster Recovery (BCDR) plans, consistent with:

- Smart Energy Code (SEC) Section H10 and Appendix AG Section 5
- The Retail Energy Code (REC) Section 9
- British Standards institute (BSI) ISO 22301 Business Continuity Management Standard
- Business Continuity Institute (BCI) Good Practice Guidelines

DCC maintains its BCDR framework to ISO22301 standards and is now accredited to that standard.

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

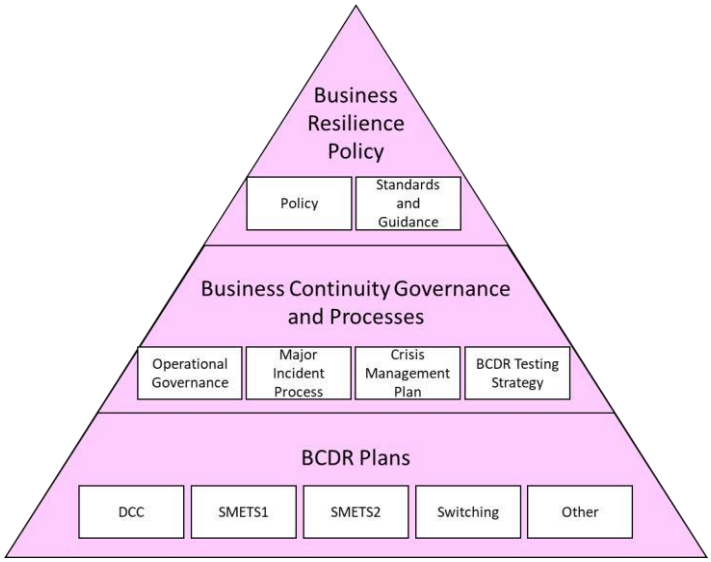


Figure 3: Business Resilience framework

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 Customers.

The Business Resilience Policy applies to both the DCC as Licensee and to all DCC Service Providers that provide services in support of the Authorised Business, including existing SMETS 1 services, SMETS2 services, 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. The outcomes of BCDR testing are reported to the SEC Panel

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.

DCC maintains a Crisis Management Team, which operates under 'Safe Harbour' principles. The team meet regularly to assess risk registers and clear operating protocols to identify a crisis and the response to the crisis.