Bank of England

Guidance to codes of practice

April 2024

Guidance to Codes of Practice

Introduction

This document sets out non-statutory guidance provided by the Bank of England (the Bank) in relation to the *codes of practice* set out in the Bank of England Wholesale Cash Distribution Recognised Persons Codes of Practice 2024.

This guidance does not purport to be a definitive guide, but aims to provide a non-exhaustive statement of the steps that a *recognised person* may take in order to comply with the above *codes of practice*.

This guidance is therefore not legally binding on *recognised persons* but the Bank will consider the extent to which a *recognised person* has complied with this guidance in assessing such *recognised person*'s compliance with the requirements of the *codes of practice*.

This guidance should therefore be read alongside and interpreted consistently with all relevant sources of law including the *codes of practice*.

This guidance is current as at the date of issue but may be revised from time to time in light of any relevant changes to legislation and to the *codes of practice* amongst other matters.

This guidance will apply from the date on which the *codes of practice* come into force.

The *codes of practice* operate in addition to the rules of the Bank of England Note Circulation Scheme (NCS). Therefore where a *recognised person* is also a member of the NCS, the person should comply with their obligations under both the rules of the NCS (the NCS Rulebook) as well as under the *codes of practice*.

Definitions

This section of the guidance provides further information on certain of the terms defined in the *codes of practice*.

The term '*cash centre*' is intended to include any facility for the storage of *cash* where the facility constitutes a premises that is owned, leased or otherwise occupied, by an *operator* for the purpose of carrying out any of the following *specified relevant functions*:

(a) undertaking;

(b) managing; or

(c) providing a service,

directly in relation to an *operational activity*.

A premises can be a *cash centre* for the purposes of the wholesale cash distribution oversight regime regardless of whether it meets any other conditions or requirements for a cash centre under the NCS. Therefore, a premises can be a *cash centre* whether the operator is a member of the NCS or not, and irrespective of whether or not the premises comprising the *cash centre* has been granted eligibility by the Bank under the NCS.

The term '*backing FI*' means a 'backing financial institution' and has been defined as 'a *recognised person* in respect of its *specified relevant function* of providing financial assistance'. This term includes financial assistance provided to the *recognised person* acting in its capacity as an *operator* such as, for example where a bank may arrange cash collection and delivery services for its banking customers and also delivers those services. The term 'financial assistance' also includes 'Settlement Agent' and 'FI Guarantor' services (as those terms are defined in the definitions section of this document as well as in the NCS Rulebook) that may be provided by a *recognised person*.

For the purposes of the *codes of practice* the Bank has introduced a definition of *operational activity*. This definition is intended to include those 'wholesale cash distribution activities' expressly mentioned in section 206E(1) of the Banking Act 2009 as well as the following activities to the extent that these may also be specified by HMT in a *wholesale cash oversight order*:

- receiving requests for *cash* from *wholesale customers*;
- preparing *cash* for distribution;
- dispatching *cash* to *wholesale customers*;

- providing *cash* collection, delivery and/or deposit services;
- reconciliation of *cash*;
- sorting of *cash*; and
- receiving *cash*.

The above definition also includes other operational *wholesale cash distribution activities* that may be specified in a *wholesale cash oversight order*.

The above terms are intended to include (but not be limited to) relevant *banknote* processing activities carried out by a *recognised person* who is also a member of the NCS and shall apply regardless of whether those relevant processing activities are carried out in respect of *banknotes* whether under the NCS or otherwise.

In particular, with respect to certain terms used in the definition of '*operational activity*' the term 'sorting of *cash*' includes activities comprising the unpacking of *cash,* the reconciliation of declared balances against *cash* actually received, the authentication of *cash*, fitness sorting, and the repacking of *cash* into containers. The term 'fitness sorting' includes the process of identifying and separating damaged cash from cash that is of sufficient quality to re-enter circulation; also known as 'fitness checking', 'quality sorting' or 'quality checking'. Where a *recognised person* who performs *specified relevant functions* in relation to the 'sorting of *cash*', is also a member of the NCS, the term 'sorting of *cash*' shall include (but not be limited to) the Sorting Process (as that term is defined in the NCS Rulebook).

The term '*wholesale collection or delivery of cash service*' is defined as 'a service whose sole or dominant purpose is the collection or delivery of *cash*'. The phrase 'collection and delivery of *cash*' includes the deposit of cash e.g. by a *wholesale customer* with a *recognised person*, or where a wholesale customer requires a deposit or dispense of cash from a *recognised person*.

The term '*wholesale customer*' is defined as a *cash services user* (as defined) who:

(a) enters into an agreement that includes the provision of a *wholesale collection or delivery of cash service*, directly with a *recognised person*; or

(b) who directly collects or delivers *cash* from or to an *operator* other than pursuant to an agreement to transport such *cash* between *operators*.

The Bank intends for paragraph (a) of the above definition to include reference (for example) to a *recognised person* acting in the capacity as a *backing FI* who enters into an agreement that includes the provision of a *wholesale collection or delivery service*, directly with a banking customer of that *backing FI*. Where a *recognised person* may act in the capacity of <u>both</u> a *backing FI* and an *operator* with respect to a *cash services user* the Bank expects that such *recognised person* would consider the *cash services user* as a *wholesale customer* of the *recognised person* acting in its capacity as *backing FI* but not as *operator*.

Certain parts of this guidance refer to ‘cash-in-transit’ or ‘CIT’ activities. The Bank defines a ‘cash-in-transit activity’ as: ‘the activity of transportation of *cash* by or on behalf of an *operator*:

(a) to or from the *issuing authorities* or the *Mint*; or

(b) between two or more c*ash centres* owned, leased or otherwise occupied by such *operator* or to or from a *cash centre* owned, leased or otherwise occupied by another *recognised person*; or

(c) to or from a *cash services user*,

whether or not such *cash-in-transit* activity is a *wholesale cash distribution activity*.

The above provisions are intended to capture *cash-in-transit* services provided to *recognised persons* in respect of the *recognised person’s specified relevant functions*. Specific provisions on such *cash-in-transit arrangements* are provided for in the *code of practice*.

Guidance to Code of Practice - Information gathering

This guidance applies to the Code of Practice – Information gathering.

References in this guidance to the *code of practice* shall be construed as references to the Code of Practice – Information gathering, unless the context indicates otherwise.

Reporting

Paragraphs 1 and 2 of the *code of practice* set out the reporting requirements for *operators* and *backing FIs* respectively.

Operators are defined in the *code of practice* as ‘a *recognised person*’ in respect of its *specified relevant functions* of:

(a) undertaking;

(b) managing; and/or

(c) providing a service in relation to,

an *operational activity*

The Bank therefore expects that *recognised persons* will comply with the reporting requirements in paragraph 1 of the *code of practice* only with respect to the *recognised person*’s functions and activities as an *operator*.

The Bank defines a *backing FI* or *backing financial institution* as a *recognised person* in respect of its *specified relevant function* of providing financial assistance.

Therefore, the Bank expects that *recognised persons* will comply with the reporting requirements in paragraph 2 of the *code of practice* only with respect to the *recognised person*’s function of providing financial assistance.

Paragraphs 1 and 2 of the *code of practice* require *operators* and *backing FIs* (as applicable) to provide the Bank with information in accordance with the WCD Data Catalogue.

Business continuity plan

Paragraph 3.1 of the *code of practice* requires each *recognised person* to draw up, test, maintain and where applicable, have appropriate regard to, a *business continuity plan*.

The *business continuity plan* must:

- identify threats or risks to the *recognised person’s* performance of its *specified relevant functions*; and

- detail how such threats and risks may be mitigated and how the *recognised person's* performance of such *specified relevant functions* will be maintained in the event of any such identified threats or risks materialising.

Paragraph 3.2 requires that the *business continuity plan* must include certain information, including:

- a business impact analysis and risk assessment;
- a business continuity strategy for the *recognised person*;
- an incident response structure;
- a testing and performance evaluation strategy; and
- any ongoing actions which need to be undertaken by the *recognised person* to ensure the *business continuity plan* is fit for purpose.

The Bank expects that the *business continuity plan* should define scenarios that represent potential threats to the operational and financial resilience of the *recognised person*, and include an outline of the procedures and instructions a *recognised person* intends to follow in the event that those threats materialise with respect to the performance by the *recognised person* of its *specified relevant functions*.

In drawing up, testing and maintaining their *business continuity plan*, *recognised persons* should have regard to the *principle* on resilience which says:

> [*Recognised persons*] *should aim to have sound business continuity and contingency arrangements in place to deal with a wide range of stress scenarios and disruptions including, but not limited to, the loss of cash processing sites, disruptions in cash transport arrangements, and changes/terminations in client and third-party supplier contractual relationships.*

The Bank therefore expects that the *business continuity plan* will incorporate all severe but plausible risk scenarios, such as:

- disruption to or failure of *cash-in-transit* activities;
- utility supply interruption (e.g. electricity, water, gas, internet, landline or mobile network connectivity);
- supply chain and distribution network disruption (including changes/termination in arrangements with *wholesale customers* and *third-party providers* including *cash-in-transit providers*, and disruptions to *cash-in-transit arrangements*);
- damage to or loss of premises (including temporary loss of a *cash centre* or other relevant cash processing site, and *cash centre* access issues including due to weather events such as snow or landslides, and other events such as disruption due to vehicular traffic incidents);
- industrial action;

- insolvency of a *third-party provider* under a *material third-party arrangement* or of a *cash-in-transit provider*;
- equipment failure;
- *recognised person*-specific cyber outage (inadvertent, malicious, or otherwise);
- market-wide cyber outage (e.g. disruption or failure of payment systems such as LINK, MasterCard, Visa);
- transport disruption (e.g. road closures);
- pandemic;
- terrorism;
- war;
- civil unrest;
- criminal proceedings being commenced against the *recognised person* or a key member of staff of the *recognised person*;
- criminal activity affecting the *recognised person's specified relevant functions*;
- key staff member vacancies or absences;
- financial distress (including insurance pay-out delays and lack of access to the services of a Settlement Agent);
- financial instability;
- social unrest;
- climate-related risks including extreme weather events (e.g. heatwaves, flooding, snow, high winds); and
- any other event comprising a sharp, short-term shock to the market such as an event occurring in the wider financial markets which could impact demand for cash, such as a chain of bank failures.

Recognised persons should also include wider climate-related risks in their assessment of potential threats to its *specified relevant functions*, including but not limited to:

- extreme weather events;
- rising sea levels;
- environmental regulatory changes;
- supply chain disruptions;
- increased insurance costs; and
- health and safety impacts.

The above examples are not exhaustive and *recognised persons* should also consider any other relevant events which could impact on the *recognised person*'s ability to carry out its *specified relevant functions*.

Where relevant, the impact of events should be considered both at a single *cash centre* and across multiple *cash centres* and, where relevant, at other critical sites such as the *relevant person's* head office and administrative branches.

Recognised persons should also consider the availability and likely effectiveness of avoiding or mitigating actions.

In particular, in the event that relevant risks are realised, the *recognised person* should consider the ease with which they could:

- move wholesale cash distribution activities, cash stocks and/or equipment between *cash centres*;
- increase operating hours; and/or
- substitute *wholesale customers* and *third party providers* (including *cash-in-transit providers*).

Recognised persons should specify in an incident response plan the particular teams/departments or single points of contact for the management of incidents covered by their incident response strategy.

Where a *recognised person* is considering the substitutability of a *cash centre*, the *recognised person* should provide the site name and address for each *cash centre* that it considers substitutable.

The *business continuity plan* should also include stress-testing of the *recognised person*'s incident response strategy.

Where assumptions are used in the *business continuity plan* these should be assumptions in which the *recognised person* has a high degree of confidence.

In addition to the above, paragraph 3.2.6 requires that the *business continuity plan* must set out the arrangements in place for the continued performance by the *recognised person* of their *specified relevant functions* in the event of a deficiency in, or disruption to, the performance of a process, service or activity, or the provision of a product or good, under a *material third-party arrangement* and any *cash-in-transit arrangement*.

The Bank intends for such arrangements to cover the period *after* any contractual or other arrangements in place with the relevant *third-party provider* have been exhausted.

Business plan

Paragraph 4.1 requires each *recognised person* must draw up and maintain a *business plan* setting out how the *recognised person* will perform their *specified relevant functions* over a period of at least two years from the date of the *business plan*.

Paragraph 4.2 sets out the information that must be included in a *business plan*. This includes:

- a description of the *recognised person*'s relevant business model and their strategy and aims; a description of the risks that will impact the day-to-day operations of the *recognised person* and: an assessment of why the risks are important and the likelihood of the risks occurring; a description of the magnitude of the potential impact of the risks occurring on the ability of the *recognised person* to perform their *specified relevant functions*; how the risks will be managed, controlled, avoided or mitigated; and the realistic availability and likely effectiveness of such managing and controlling, avoiding or mitigating actions; an assessment of the viability and resilience of the business; and
- a description of any material challenge to the resilience of the *recognised person*'s ability to carry out its *specified relevant functions* over the term of the business plan, together with an explanation of how they have arrived at this judgement of materiality.

A business plan should describe the business with regard to the *specified relevant functions* of the *recognised person*, and should include the *recognised person*'s objectives, strategies, sales, and financial forecasts in this regard.

*Recognised person*s may wish to refer to the UK Corporate Governance Code and industry guidance thereto, in considering the nature and scope of their business plan, and should interpret terms such as ‘business model’ and ‘strategy and aims’ in accordance with the Code and such guidance.

In particular, an assessment of the viability and resilience of the business should include both the financial and operational resilience of the business.

With respect to the risk assessment referred to in paragraph 4.2.5 of the *code of practice*, *recognised persons* should:

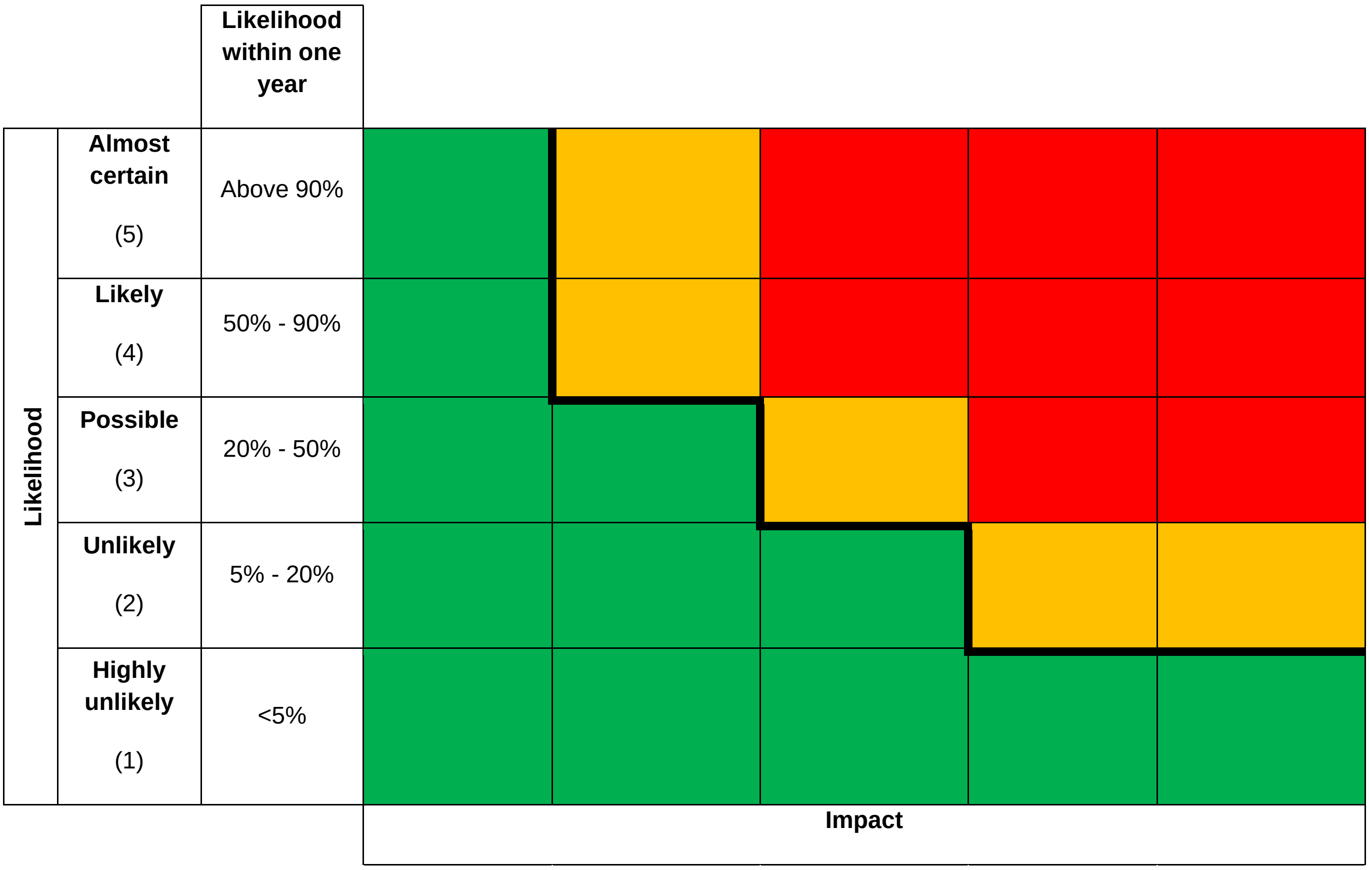
- only include assumptions that are made by the *recognised person* with a high degree of confidence;
- assess the risks to the business model, future performance, solvency and liquidity of the *recognised person* in respect of its performance of its *specified relevant functions*
- include both qualitative and quantitative analysis of risks;
- analyse any trends of the risks and threats to the recognised person's performance of its *specified relevant functions*, including long-term risks; and
- include real-time insight as well as a long-term perspective on risks.

The analysis should be tailored to the specific circumstances of the *recognised person* (taking into account its position in the relevant market, its performance, its business model, business plan, strategy, and principal risks) and be undertaken with prudence (that is weighting downside risks more heavily than upside opportunities).

Recognised persons should consider the impact on their business model of climate change. This should include the impact of:

- reducing the contribution of their specified relevant functions to climate change; and
- adapting to and mitigating the impact of climate change on their specified relevant functions.

A *recognised person* should assess the impact and likelihood of risk scenarios using the heat map and harm table below as a guide, and evaluate the likely impact on the *recognised person*'s *specified relevant functions* of such events crystallising.



Impact:	**Little / none** (1)	**Minor** (2)	**Moderate but short term** (3)	**Considerable but short term** (4)	**Substantial and / or sustained** (5)

Financial losses		To be set by recognised person	To be set by recognised person	To be set by recognised person	To be set by recognised person	To be set by recognised person
Operational disruption		Local impact or impacts a key task	Non-critical business activity / system / process impacted	Business-critical process (or critical supporting process/ system) impacted	Business-critical function impacted	Substantial and / or sustained operational impact preventing *the recognised* person from fulfilling its functions
	Materially beyond tolerance	Urgent and / or significant mitigating action required.				
	Just out of tolerance	Some mitigating action required.				
	In tolerance	Managed at local level.				

Self-assessment

Paragraph 5 provides that, in respect of each calendar year (or part thereof) each *recognised person* must complete a written *self-assessment* that sets out how the *recognised person* has had regard to the *principles* in the performance of their *specified relevant functions*; and complied with each *code of practice*, in respect of such year (or part thereof).

References to ‘parts thereof’ of a calendar year, refer to the initial period for self-assessment where the *recognised person* submits their first self-assessment to the Bank.

Recognised persons are expected to make their own determination as to the form that their self-assessment document should take and the level of detail to be included in the document, taking into account the extent to which the *recognised person* has met the Bank’s expectations and requirements under the *principles* and the *codes of practice*.

The *self assessment* may be submitted together with the written attestation (referred to below) in accordance with the requirements of the *code of practice*.

Service level agreements

Paragraph 6 provides that each *recognised person* must take appropriate steps towards measuring the performance by it or on its behalf, of its *specified relevant functions*.

Recognised persons should refer to Annex 1 (*Providing Service Level Agreement Data*) to the WCD Data Catalogue for guidance as to what the Bank considers would be ‘appropriate steps’ towards measuring the performance by a *recognised person* of its *specified relevant functions*.

Sustainability

Paragraph 7 requires that each *recognised person* must put in place appropriate arrangements for the setting of targets, and for the monitoring of performance against such targets, in relation to the sustainability of its *specified relevant functions.*

Recognised persons should refer to Annex 3 (*Setting Sustainability Targets*) to the WCD Data Catalogue for guidance as to what the Bank considers would be ‘appropriate arrangements’ for the setting of targets and for the monitoring of performance against such targets, in relation to the sustainability of a *recognised person’s specified relevant functions.*

Annex 3 also sets out the scope of what the Bank considers to be the ‘sustainability’ of a *recognised person’s specified relevant functions*.

Attestation

Paragraph 8 provides that as at the last day of each calendar year each *recognised person* must complete a written attestation that the information that the *recognised person* has provided to the Bank pursuant to any of the *codes of practice* (taking into account any information that the Bank has notified to the Bank under event notification and information update requirements of the *codes of practice*) is complete, accurate and up to date.

Recognised persons must submit the written attestation to the Bank in accordance with the information submission provisions of the *code of practice*.

Wholesale customer pricing

Paragraph 9 requires *recognised persons* to collate ‘appropriate details’ of the fees and charges charged by the *recognised person* to *wholesale customers* in respect of the *recognised person’s specified relevant activities*.

Such ‘appropriate details’ will include the creation of a standard pricing tariffs document, which details the typical charges levied on *wholesale customers* for the performance of the *recognised person’s specified relevant functions*.

Recognised persons should refer to the WCD Data Catalogue for further guidance as to what the Bank considers would be ‘appropriate details’ of the fees and charges referred to in paragraph 9.

Information reporting framework

Paragraph 11 provides that each *recognised person* must ensure that appropriate arrangements are in place for the management of information relating to the performance of their *specified relevant functions.*

Such 'appropriate arrangements' could include the following:

- individuals would be appointed as a 'data owner', a 'data steward' and a 'data expert' on behalf of the *recognised person*.
- The 'data owner' and 'data steward' roles should be held by individuals who are employed by the *recognised person* in the business areas or departments associated with the *recognised person's* participation in the wholesale cash distribution market oversight regime.
- A single individual should not hold more than one role as a 'data owner', 'data steward' or 'data expert' at any one time.
- The individuals would each be appropriately qualified for the role and would have the attributes and responsibilities referred to below.

Data owner[1]

A member of the governing body or senior management of the *recognised person who:*

- works in the business area that compiles and submits information to be provided to the Bank;
- is accountable within the *recognised person* for decisions made in relation to the information to be provided to the Bank and has the authority within the *recognised person* to make decisions with respect to the information; and
- has sufficient an understanding of the information to be provided to the Bank in order for the *recognised person* to be able to attest that the *recognised person* complies with the Bank*'s* information requirements.

---

[1] The decision hierarchy below may assist the *recognised person* in determining who the data owner should be:

1. Which department is most critically responsible for the dataset and has most to lose from it not being available?
2. Who uses the dataset most intensively?
3. Where are the data subject matter experts located?
4. Who pays for it or has commissioned its creation?
5. Which area will users naturally expect to take responsibility?
6. Where is the data steward located?

When appropriate, the data owner may delegate some of their responsibilities to a data steward and data experts.

A *recognised person* should appoint only one data owner at any one time.

Data owner responsibilities

(a) Decision-making

- Sponsor or approve the need for the acquisition, creation, and ongoing curation of datasets of information required to be provided to the Bank.
- Decisions within the remit of the data owner may include matters such as retention, confidentiality, storage and access requirements relating to information to be provided to the Bank.
- Mobilising resources within their team and data boards including appointing data stewards and data experts where required.

(b) Standards and compliance

- Ensure data is used in accordance with the *recognised person*'s policies where these apply.
- Ensure data is collected, used and disposed of according to internal standards as well as laws and regulations e.g. the *recognised person's* data and security policies, and government regulations and data protection legislation.
- Ensure the dataset is appropriately classified in accordance with the *recognised person's* information security classification scheme if applicable.
- Ensure potential data risks are identified, communicated, and measures such as the *recognised person's business continuity plan* is in place.

(c) Data management

- Promote and sponsor good data quality practice and ongoing data quality improvements to help ensure data is fit-for-purpose.
- Ensure the data is registered in the *recognised person* as a known data asset by oneself or a nominated data steward. This aids awareness and data discovery, and also minimises risk of having unknown and untrusted data.
- Establish retention or disposal of the data in accordance to the *recognised persons*' records classification scheme or equivalent documentation, and in accordance with data protection legislation.
- Ensure individual/team supporting data governance activities are appropriately trained.

(d) Managing data risk

- Enabling the conditions for data to be stored, used and accessed safely; in line with any confidentiality, privacy, compliance, legal, regulatory or security requirements as set out by the relevant areas in the *recognised* *person*. Facilitate the process to authorise and validate requests for accessing, sharing and submitting the dataset.

- Have lines of communication established so they are informed by their team or recipients of their data of any issues regarding the data.

(e) Change management

- Facilitate ongoing curation and change by sponsoring and mobilising sufficient resource to address enhancements and fixes to the data.

Data steward

Appointed by the data owner, data stewards are responsible for the day-to-day data governance activities / responsibilities assigned or delegated to them by the data owner. This includes maintaining quality data; and as experts in the data and its use, understanding the requirements that data needs to meet to be fit for purpose.

Given the data steward's role in supporting the data owner, the data steward will typically report to the data owner. Where this is not case, it is recommended that a formalised arrangement is established to document and agree the split of responsibilities between the data steward and data owner.

A *recognised person* should appoint only one data steward at any one time.

<u>Data steward responsibilities</u>

(a) Dataset knowledge & documentation

- Maintain metadata and documentation for the dataset.
- Understand the detail of the inputs and outputs involved in the supervisory reporting. Details include key users, definitions, source data legal authority or status, where it is stored, how to access, procedures for updating etc.
- Record of log of events or decisions that have impacted the dataset, to support audit.

(b) Delivery

- Undertake / ensure data quality is monitored, with appropriate controls and remediation activities identified and as needed prioritised / escalated for remediation.
- Work with the Bank to identify and address potential data quality issues.
- Support in the definition and design of process, standards and procedures and controls.
- Ensure changes to data collections and new collections are implemented.

(c) Incident Management

- Deal with and oversee data queries from users, stakeholders or the Bank, requesting advice from data experts where necessary.

- Collect, collate and triage issues and problems with the dataset.
- Prioritise and communicate issues and incidents to stakeholders who are impacted as well as who can support remediation efforts, e.g. the data owner and the data experts.
- Provide support and ensure the completion of remediation efforts.

(d) Policy Adherence

- Review the compliance of the dataset with data management policies and standards.
- Inform the relevant data owner and stakeholders when risks or conflicts arise.

(e) Administration

- Be the point of contact for other users across the *recognised person* who have questions on the dataset. Escalating issues to the data owner where appropriate.
- Oversee and provide advice on data queries from the Bank.

Data expert

Data experts are roles that operate in addition to the data steward.

The data expert may be an individual who works closely with the data or with the data owner or the data steward. Data experts may be an individual from a different team or department to that in which the data owner or data steward work, or may be an individual who has worked with the dataset over a period. Typical job titles for a data expert include Data Analyst, Data Scientist or Policy Analyst.

A *recognised person* may consider appointing more than one data expert.

Data expert responsibilities

- Provide technical expertise to understand, interpret and compile the supervisory reporting.
- Provide support and knowledge to internal and external stakeholders.
- Communicate data issues and incidents to the data steward and the data owner.
- Perform data remediation within specified time periods as required.
- Promote good data governance/management/data quality practices and policies.
- Undertake data steward responsibilities in absence of a data steward when required.

Guidance to Code of Practice - Third-party arrangements

This guidance applies to the Code of Practice – Third-party arrangements.

References in this guidance to the *code of practice* shall be construed as references to the Code of Practice – Third-party arrangements, unless the context indicates otherwise.

Arrangements

The definition of *arrangement* in the *code of practice* includes arrangements in any form. Arrangements would not need to be in writing to fall within the scope of the definition. Arrangements are likely to fall within the scope of the definition even where they may not constitute a legally binding agreement or contract between a *recognised person* and a *third-party provider*.

Third-party arrangements

The definition of *third-party arrangement* includes both products and goods as well as processes, services and activities provided by a *third-party provider*. It can also include *arrangements* where the *third-party provider* is a member of the same *group* as the *recognised person* with whom the *arrangements* are made.

The Bank expects that products and services within scope of a *third-party arrangement* will include:

Arrangement Type	**Examples of products and services**
Cash Processing Equipment (for notes and coin)	A *third party provider* materially involved in the sourcing, production, maintenance, and upgrade of cash-handling machinery. • High Speed or bulk sorters • Medium Speed sorters • Machine sensors (Authentication and fitness e.g. infra-red or magnetic sensors for notes and High Security Features (HSF) for coin) • Desktop counters/sorters • Hardware and software maintenance/updates • Stripping, packaging/bagging/banding equipment • Weighing Scales for check weighing • Intelligent Safes • Local recycling equipment • Apparatus for moving banknote/coin cages (Pallet loaders)
Cash in Transit	A *third party provider* materially involved in *cash-in-transit* and/or:

	• Trunking of banknotes and coin between cash centres and issuing authorities • Cash transport to and from wholesale customers • Ownership and upkeep of cash-in-transit vehicles
Cash Packaging	A *third party provider* materially involved in the sourcing or production of cash packing materials. • Containers (Safebags, Coin tubes, single use/reusable bags) • banknote/boin cages • Labelling • Security seals • Wrappers/film
IT Services	A *third party provider* materially involved in the sourcing, production, maintenance, and upgrade of IT hardware and software required for delivery of 1 or more operational activities. • Cash inventory management systems; • Wholesale customer order handling; • Remote monitoring – site security, vehicle tracking/management; • Secure telecommunications providers; • End-user computing services; • Back office applications - change management, backups and disaster recovery • Access to Bank of England & Royal Mint stock management & reporting systems
Upkeep of Security Measures	A *third party provider* materially involved in the sourcing, production, maintenance, and upgrade of cash security equipment and services. • Monitoring (CCTV, alarms, security teams, vetting providers) • Perimeter protection (Gates, barriers, fences) • Internal entry systems (Vault & 'airlock' doors, turnstiles, biometrics, key safes) • Health and safety (Ventilation, heating & cooling, fire & carbon monoxide monitoring and suppression systems) • Vehicles (CIT adaptations, security countermeasures such as foam, glue and dye protections) • Asset protection (Banknote/Coin cages, ATM cassettes, cage seals and packing materials, CIT & cash centre insurance)
Financial Services	A *third party provider* who provides financial services required for the recognised person’s involvement in 1 or more operational activities. • Insurance coverage (Premises, transport, personnel) • Collateral facilities • Liquidity facilities • Settlement facilities (Including access to the Bank’s Real-time Gross Settlement (RTGS) system)
Cash Handling	A *third party provider* who is materially responsible (wholly or in-part) for carrying out 1 or more operational activities on behalf of the recognised person.

	• Cash Storage • Cash Processing (Reconciliation, Authentication, Fitness Sorting)

Materiality assessments

Paragraph 1.1 of the *code of practice* provides that before entering into a *third party arrangement*, a *recognised person* must carry out a materiality assessment in respect of that *third-party arrangement*.

The Bank expects that the materiality assessment would take place before the *recognised person* becomes legally bound by or otherwise committed to the *third party provider* in respect of such arrangements.

A materiality assessment involves the exercise of judgment about the financial and operational impact that the provision of the product or services could have on the ability of the *recognised person* to perform its *specified relevant functions* as set out in the wholesale cash distribution order made in respect of it, and in relation to the performance of the particular wholesale cash distribution activities that have been specified for it in that order.

Recognised persons should develop their own approach to assessing the materiality of their *third-party arrangements*. However *recognised persons* should take into account both quantitative and qualitative criteria in their materiality assessments.

The Bank expects *recognised persons* to conclude that at least one *arrangement* from the table above is a *material third-party arrangement*. Details of these arrangements will be provided as part of the Material Third-Party Arrangements data item as detailed in the WCD Data Catalogue. Where a *recognised person* does not conclude that an *arrangement* from the table above is a *material third-party arrangement*, they should be prepared to explain the reasons for this.

<u>Quantitative criteria</u>

The quantitative criteria for the materiality assessment required pursuant to paragraph 1.1 should set out:

- the percentage of the cash volumes (where cash volume is expressed in total number of Bank*notes* and *coin*) that rely directly or indirectly on the *third-party provider*;
- how many *specified relevant functions* are directly or indirectly affected by the *third-party provider*. Where appropriate this should be split out by product and service; and
- any other quantitative factors that could affect the materiality of a *third-party provider*.

<u>Qualitative criteria</u>

Qualitative criteria are factors relating to the overall importance of a *third-party arrangement* to the ability of the *recognised person* to perform their *specified relevant functions*. The qualitative criteria should be the primary consideration.

Recognised persons should consider:

- the extent to which the *recognised person* depends on the product or service to perform its *specified relevant functions*;
- in the case of *third-party arrangements* for the provision of a process, service or activity, the extent to which the *third-party provider* could be replaced by or substituted with an alternative provider in the relevant market for the services (including the extent to which the *recognised person* could perform the relevant service for itself) if such *third-party provider* were to become insolvent or to otherwise no longer perform the services for the *recognised person*;
- in the case of *third-party arrangements* for the provision of a product or good, the supply chain for such delivery;
- the extent to which the product or service could be replaced by or substituted with an alternative product or service; and
- any other qualitative factor that could affect the materiality of a *third party provider*.

Ultimately the *recognised person* should have regard to all relevant factors that may impact its ability to perform its *specified relevant functions*.

Materiality may vary throughout the duration of a *third-party arrangement* and should therefore be reassessed:

- at appropriate intervals e.g., during scheduled review periods;
- where a *recognised person* proposes to scale up its use of the product or service or its dependency on the *third-party provider*;
- where there is a material change in the circumstances of the *recognised person* or the *third-party provider* or the nature or scope of the product or service; and
- where the *recognised person* becomes aware during the lifetime of the *third-party arrangement*, of new information relevant to its materiality assessment.

Due diligence

Paragraph 1.2(1) of the *code of practice* provides that before entering into a *material third-party arrangement*, a *recognised person* must carry out appropriate due diligence in respect of the proposed *third-party provider*.

<u>Products and goods</u>

In the case of *material third-party arrangements* for the provision of a product or good, the Bank expects *recognised persons*' due diligence to consider:

- the supply chain arrangements of the potential *third-party provider*; and
- the extent to which the *third-party provider* promotes sustainable practices in its relevant business, in line with Government climate-related policies and standards.

<u>Services</u>

In the case of *third-party arrangements* for the provision of a process, service or activity, the Bank expects *recognised persons*' due diligence to consider the potential *third-party provider's*:

- creditworthiness;
- business model, complexity, financial situation, nature, ownership structure, and scale;
- capability, expertise, and reputation;
- financial, human, and technology resources;
- information and communication technologies (ICT) controls and security; and
- sub-contracted service providers, if any, that will be involved in the performance of the *specified relevant functions*.

The due diligence should also consider whether potential *third-party providers*:

- can comply with applicable legal and regulatory requirements to perform the service;
- comply with data protection legislation;
- can demonstrate certified adherence to recognised, relevant industry standards;
- can provide, where applicable and upon request, relevant certificates and documentation;
- have the ability and capacity to provide the service that the *recognised person* needs in a manner compliant with UK regulatory requirements (including in

the event of a sudden spike in demand for the relevant service, for instance as a result of a shift to remote working during a pandemic). A ‘general’ track-record of previous performance may not be sufficient evidence by itself; and

- have appropriate arrangements in place to continue to perform the services in the event of changes in the price of relevant commodities (such as oil prices) and in interest rates.

The *recognised person*’s due diligence in respect of a *third-party provider* should be reassessed in the same circumstances as when a materiality assessment is completed and also if a significant organisational change at the *third-party provider* or in any *person* on whom the *third-party provider* is dependant for the provision of products or services to it, takes place, that could materially change the nature, scale, and complexity of the risks inherent in the *third-party arrangement* (such as a significant change to the *third-party provider’s* ownership or financial position).

Risk assessment

Paragraph 1.2(2) of the *code of practice* provides that before entering into a *material third-party arrangement*, a *recognised person* must carry out an appropriate risk assessment in respect of a *material third-party arrangement*.

Recognised persons should, therefore, in a proportionate manner, assess the potential risks of *material third-party arrangements* relevant to the performance of *the recognised person’s specified relevant functions*.

As part of the *risk assessment*, the Bank expects *recognised persons* to consider:

- operational risks based on an analysis of severe but plausible scenarios, for instance a breach or outage affecting the confidentiality and integrity of sensitive data and/or availability of the service provision;

- financial risks, including the potential need for the *recognised person* to provide financial support to a *third-party provider* in distress or to take over its business, including as a result of an economic downturn (‘step-in’ risk);

- concentration risks based on the availability of the product or service in the relevant market and the ability to move to a new *third-party provider*;

- risks to the effectiveness, resilience and sustainability of wholesale cash distribution throughout the United Kingdom and throughout any part of the United Kingdom; and

- existing or planned risk mitigation, e.g., staff procedures and training.

The Bank expects *recognised persons* to conduct appropriate due diligence on the potential *third-party provider* before entering into a *material third-party arrangement*, and to identify a suitable alternative or back-up provider(s) where available.

If no alternative or back-up provider for a *material third-party arrangement* are available, recognised persons should consider alternative business continuity, contingency planning, and disaster recovery arrangements to ensure that there is no significant deficiency in, or disruption to, the performance of such services, that would be likely to undermine the ability of the *recognised person* to perform its *specified relevant functions*.

The *recognised person's* risk assessment should be reassessed in the same circumstances as when a due diligence reassessment is completed and also in circumstances where there has been a significant change to a *third-party providers'* risks due to, for instance, a serious breach or continued breaches of the relevant *material third-party arrangement* or a risk that has crystallised.

A *recognised person's* risk assessment should balance any risks that the *material third-party arrangement* may create or increase against any risks it may reduce or mitigate e.g., by enabling the *recognised person* to manage overall risks more effectively.

Recognised persons should comply with their obligation to carry out a risk assessment in respect of a *material third-party arrangement*, in a manner appropriate to the *recognised person's*: size and internal organisation; the nature, scope, and complexity of their *specified relevant functions*; and the criticality or importance of the *material third-party arrangement*, in line with the principle of proportionality.

Material third-party arrangements

Paragraph 2(1) of the *code of practice* requires that *recognised persons* must ensure that each *material third-party arrangement* contains appropriate provisions to ensure the delivery of the process, service, activity, product or good, such that any deficiency in, or disruption to, the performance of such process, service or activity, or any deficiency in, or disruption to, the provision of such product or good, would not be likely to significantly undermine the ability of the *recognised person* to perform a *specified relevant function*.

Recognised persons should ensure that its *material third-party arrangements* are set out in writing and include provisions governing:

- whether the sub-contracting of a service or part thereof is permitted and, if so, under which conditions. Contracts should require the *third-party provider* to notify the *recognised person* of any sub-contracting arrangements where applicable;
- the accessibility, availability, integrity, confidentiality, privacy, and safety of relevant data;
- policies and procedures to identify, address and manage conflicts of interest;

- the right of the *recognised person* to monitor the *third-party provider's* performance on an ongoing basis (this may be by reference to service level agreements or key performance indicators);
- the agreed service levels, which should include qualitative and quantitative performance criteria and allow for timely monitoring, so that appropriate corrective action can be taken if these service levels are not met;
- the reporting obligations of the *third-party provider*, including a requirement to notify the *recognised person* of any development that may have a material adverse impact on the *third-party provider's* ability to effectively perform the *specified relevant function* in line with the agreed service levels and in compliance with applicable laws and regulatory requirements;
- whether the *third-party provider* should take out insurance against certain risks and, if applicable, the level of insurance cover requested;
- the requirements for both parties to implement and test business contingency plans. Where appropriate, both parties should commit to take reasonable steps to support the testing of such plans;
- ensuring that data owned by the *recognised person* can be accessed promptly in the case of the insolvency, resolution, or discontinuation of business operations of the *third-party provider*;
- an obligation of the *third-party provider* to co-operate with the Bank and further provisions required pursuant paragraphs 2(2) and (3) of the *code of practice*;
- rights of the *recognised person* to inspect and audit the *third-party provider* with regard to the *material third-party arrangements*;
- appropriate and proportionate information security related objectives and measures, including requirements such as minimum ICT security requirements, specifications of *recognised person*s' data lifecycles, and any requirements regarding to data security, network security, and security monitoring processes and operational and security incident handling procedures, including escalation and reporting; and
- termination rights and exit strategies covering both stressed and non-stressed exit scenarios. As in the case of business contingency plans, both parties should commit to taking reasonable steps to support the testing of the *recognised persons'* termination plans. *Recognised persons* may consider limiting contractual termination rights to situations such as: material breaches of law, regulation, or contractual provisions; those that create risks beyond their risk tolerance; or those that are not adequately notified and remediated in a timely manner.

Paragraph 2(2) of the *code of practice* provides that *recognised persons* must ensure that a *material third-party arrangement* waives any contractual or other duty of confidentiality owed by the *recognised person* to the *third-party provider* which might limit the provision of information by the *recognised person* to the Bank in accordance with any *code of practice*.

Paragraph 2(3) requires that a *material third-party arrangement* must not otherwise impair the ability of the Bank to exercise its powers under Part 5A of the Banking Act 2009 in respect of the performance by the *recognised person* of a *specified relevant function*.

In addition to the above, r*ecognised persons* should ensure that a *material third-party arrangement* does not impair the ability of the *recognised person* to act in accordance with the rules of the *note circulation scheme* where such rules are applicable to the performance by the *recognised person* of a *specified relevant function*.

Recognised persons should also take reasonable steps to ensure a *third-party provider* under a *material third-party arrangement*:

- acts in accordance with the NCS rulebook where applicable;
- deals with the Bank in an open, co-operative and timely way in the discharge of the Bank*'s* functions in relation to the *recognised person's specified relevant functions*; and
- permits any representative or appointee of the Bank to have access to any of its business premises, in relation to the discharge of the Bank*'s* functions in accordance with the WCD legislative framework.

In complying with their obligations under the *code of practice*, *recognised persons* should have regard to the *principles,* which are set out in the Statement of Policy.

Cash-in-transit arrangements

The Bank considers that *cash-in-transit* activities have a particular importance in the wholesale cash distribution market, including where *cash-in-transit* services are provided to *recognised persons* in the carrying on by such *recognised persons* of their *specified relevant functions*. Given the importance of *cash-in-transit* activities to the WCD industry, the Bank has set out specific requirements for *cash-in-transit* arrangements provided to *recognised persons* in the Code of Practice – Third-Party Arrangements.

Paragraph 1.3 provides that before entering into any *cash-in-transit arrangement*, a *recognised person* must carry out appropriate due diligence in respect of the proposed *cash-in-transit provider*; and carry out an appropriate risk assessment in respect of such *cash-in-transit arrangement*.

Paragraph 1.3 is intended to apply to arrangements with any *cash-in-transit provider* regardless of the materiality of the provider.

Recognised persons should consider the guidance provided above in respect of *material third party arrangements* in carrying out due diligence and a risk assessment of a *cash-in-transit provider*.

Paragraph 3 requires *recognised persons* to ensure that any *cash-in-transit arrangement* meets the requirements set out in that paragraph. In addition to the requirements of that paragraph, *recognised persons* should also apply to its *cash-in-transit arrangements* the guidance provided above for *material third party arrangements*.

Governance

Recognised persons should ensure that their board of directors or other management body approves the materiality assessments, due diligence and risk assessments referred to above.

Recognised persons who enter into *arrangements* with *third-party providers* remain fully accountable for complying with all their obligations under the wholesale cash distribution oversight regime.

Recognised persons' boards are expected to have processes and procedures in place to ensure the effective management of all risks to which the *recognised person* is exposed including by appropriately identifying and having an understanding of the *recognised person's* reliance on *third-party providers*; and by ensuring that the *recognised person* has appropriate and effective risk management systems and strategies in place to deal with their obligations in respect of *third-party providers*.

Management information on *material third-party arrangements* should be provided to the board and should be clear, consistent, robust, timely, and well targeted, and contain an appropriate level of technical detail to facilitate effective oversight and challenge by the board.

Record-keeping

Recognised persons should keep a record of the assessments and due diligence that they are required to carry out pursuant to the *code of practice*.

Guidance to Code of Practice on Cash Centre Closure and Market Exit

This guidance applies to the Code of Practice – Cash centre closure and exit.

References in this guidance to the *code of practice* shall be construed as references to the Code of Practice – Cash centre closure and exit, unless the context indicates otherwise.

Definitions

The definition of *cash centre closure* is intended to include any reduction in scope of the performance of a *specified relevant function* in relation to an *operational activity* at a *cash centre* such as where an *operator* proposes to scale back their relevant operations at, or to close only part of, a facility and where an *operator* intends to 'mothball' all or part of a site, or to convert the site to an alternative use. The definition is intended to include a *cash centre closure* that is either temporary or permanent.

The definition of *exit* is intended to include any reduction in, or winding down of, a *specified relevant function* (such as a cessation in the provision of financial assistance by a *financial institution* to an *operator* in relation to a wholesale cash distribution activity) other than where the proposal would constitute a *cash centre closure*. Where a *recognised person* performs only relevant *wholesale cash distribution activities* in relation to a *cash centre* (such as, for example, storing *cash*, dispatching *cash*, sorting *cash* and undertaking authentication processes, from a *cash centre*) and proposes to cease performing all of those activities, the Bank would regard that proposal as within the scope of the definition of *cash centre closure* and not *exit*. In such a case the *recognised person* would only need to notify the Bank of the proposed *cash centre closure* under paragraphs 1.1 and 1.2 of the *code of practice* and would not need to also notify the Bank under paragraph 2.1 of any proposed *exit*.

There is no minimum requirement for, or materiality threshold in, the definition of *exit* and, as such, the Bank would expect to be notified of all proposals to cease performing a *specified relevant function*, including proposals to cease performing only part of a *specified relevant function*. The definition is intended to include an *exit* that is either temporary or permanent.

Notification of *cash centre closure*

<u>Notification</u>

Paragraphs 1.1 and 1.2 of the *code of practice* requires *operators* to notify the Bank of their intention to effect a *cash centre closure* at the earliest opportunity and no

less than six months in advance of the date on which the *cash centre closure* is intended to take place.

Paragraph 1.3 requires notification of a *cash centre closure* to include certain information, including:

- an assessment of the impact of the *cash centre closure* on the ability of the *operator* to perform its *specified relevant functions*;
- measures that appear to the *operator* to be necessary or expedient to address any potential deficiency in, or disruption to, the performance by the *operator* of its *specified relevant functions*, including details of any actions already taken;
- a cost benefit analysis of the *cash centre closure*;
- the timeframe for implementation of the *cash central closure*;
- the likely barriers to implementation of the *cash centre closure*;
- a description of: (a) the stakeholders (including any *backing FIs* and any other *operators*) likely to be impacted by the *cash centre closure*; and (b) the actions that the *operator* has taken or intends to take in relation to such stakeholders;
- the communication strategy for the *cash centre closure*;
- the job title and a description of the responsibilities of each individual designated as having responsibility for and being accountable to the *governing body* of the *operator* for, oversight of the implementation, production, review and sign off of the *cash centre closure*; and;
- an explanation of how the *operator* has had regard to the *principles* in preparing certain of the information required by paragraph 1.3.

<u>Impact assessment</u>

An assessment of the impact of a proposed *cash centre closure* on the ability of the *operator* to perform its *specified relevant functions* (the impact assessment) should include:

- a quantitative and qualitative assessment of the impact of the proposal on the *operator's specified relevant functions*;
- a description of the way in which the proposal will affect the *operator's*:
    - business impact analysis and risk assessment;
    - business continuity strategy;
    - incident response structure; and
    - testing and performance evaluation strategy;
- a description of the way in which the proposal will affect the:
    - *operator's* business model;
    - *operator's* strategy and aims;
    - markets in which the *operator* operates;

  - *wholesale customers* of, and *third-party providers* to, the *operator*;
  - day to day operations of the *operator*; and
  - viability and resilience of the *operator*;
- an analysis of the extent to which the proposal will affect the ability of the *operator* to comply with its contractual and other obligations, and with any *service level agreements* in place for it;
- a description of the extent to which the proposal will affect the wider wholesale cash distribution industry, including an assessment of the extent to which the existing facilities and operations of the *operator* can absorb the functions and activities of the *cash centre*; and
- the operational impact of the proposal including the impact on any ongoing business operations, shareholders, providers of funding (including unsecured creditors), and support functions.

Operators must have regard to the *principles* in carrying out their impact assessment (amongst other matters).

<u>Risk mitigation</u>

Operators must consider measures that appear to them to be necessary or expedient to address any potential deficiency in, or disruption to, the performance by the *operator* of its *specified relevant functions*, including details of any actions already taken (risk mitigation measures).

These include:

- a description of the realistic alternatives to the provision of *relevant functions* at the *cash centre*;
- a description of any risk mitigation strategies that the *operator* intends to put in place to reduce the impact of the proposed *cash centre closure* on the *operator's specified relevant functions* and on the wider wholesale cash distribution market.

The execution of each option should be credible. *Operators* should consider the systemic implication of each option – and potential combinations of options – on the wider wholesale cash distribution market.

<u>Cost benefit analysis</u>

Paragraph 1.3(5) requires *operators* to provide a cost benefit analysis in respect of a proposed *cash centre closure.*

The Bank expects that such analysis would comprise: (a) an analysis of the costs together with the analysis of the benefits that would arise if the proposal is implemented; and (b) an estimate of those costs and benefits, and would include:

- an assessment of the projected (i) costs and expenses and (ii) cost savings and other benefits, in each case to (a) the *operator* and (b) any other person or organisation, arising from the *cash centre closure*;
- a description of the projected benefits of the *cash centre closure* on the effectiveness, resilience and sustainability of the wholesale cash distribution industry;
- a description of the projected disadvantages of the *cash centre closure* on the effectiveness, resilience and sustainability of the wholesale cash distribution industry; and
- taking into account the above factors, an assessment of the overall financial and other impacts of the *cash centre closure* on the wholesale cash distribution industry.

Operators should ensure that their assessment of the projected (i) costs and expenses and (ii) cost savings and other benefits, includes the costs of any redundancy or severance pay of *employees*, any early termination payments due under a lease or contract (including any break costs or exit fees), costs relating to the establishment of alternative facilities to provide alternative access arrangements, as well as anticipated costs savings.

Operators should apply commercial valuation and accounting principles to their calculation of the costs and benefits of the proposal and should provide such information as would enable the Bank to understand the rationale for the proposal and the relative costs and benefits of the options available to the *operator* to continue to meet the needs of its *wholesale customers*.

<u>Timeframe</u>

Paragraph 1.3(6) requires *operators* to provide the Bank with information about the timeframe for implementation of the *cash centre closure*.

Information about the timeframe should include:

- the date on which the *operator* intends to effect the *cash centre closure*;
- a description of the key milestones and main phases for implementation of the *cash centre closure*, and the dates for these, including:
    - identification of notification and communication requirements in respect of all stakeholders likely to be affected by the *cash centre closure* such as, for example, notification periods for termination of a lease or other contract relating to the *cash centre,* and any requirements for consultation about the proposal with employees;
    - consideration of any regulatory requirements (such as, for example, of the Financial Conduct Authority, the Payment Systems Regulator or the Prudential Regulation Authority) in relation to the *cash centre closure* and a description of the timeframes for these;

  - consideration of any notification obligations (such as, for example, market disclosure obligations) and the timeframe for these;
  - consideration of any contingencies or variables in the implementation of the proposal for *cash centre closure* and a description of how these could affect the timeframe for implementation;
  - a description of the *operator's* internal governance and the steps necessary to effect the proposal and the timeframe for these; and
  - how the likely barriers to implementation of the *cash centre closure* identified pursuant to paragraph 1.3(7) of the *code of practice* could impact the proposed timeframe for implementation.

Operators should also ensure they consider whether it is necessary or desirable to engage with His Majesty's Treasury (HMT) in relation to the *cash centre closure,* including considering whether an amendment to the *operator's wholesale cash distribution order* would be required.

Operators should provide the Bank with a copy of any communications they have with HMT in respect of a *cash centre closure*.

Operators should provide the Bank with a progress report at each key stage of the implementation.

Barriers to implementation

Paragraph 1.3(7) requires *operators* to inform the Bank of the likely barriers to implementation of the *cash centre closure*.

Such barriers to implementation could include dependencies or contingencies such as: the potential for any sale of an asset to fall through (in the case of a *cash centre closure* that arises from a proposed sale of all or part of an *operator's* business); the potential for a regulatory or planning approval to be refused; requirements for actions to be taken in relation to a contract (e.g. notice to be provided); and operational considerations.

Stakeholders

Paragraph 1.3(8) requires *operators* to provide the Bank with a description of: (i) the stakeholders likely to be impacted by the *cash centre closure*; and (ii) the actions that the *operator* has taken or intends to take in relation to such stakeholders.

The term 'stakeholders' includes:

- *wholesale customers* of an *operator*;
- *third-party providers* to the *operator*;
- *employees* of the *operator* and any trade union representing such *employees*;
- the landlord where the *operator* holds a leasehold interest in a *cash centre*;
- providers of financial assistance in relation to the *cash centre*;

- any other person or organisation with whom the *operator* has a contractual or other relationship (e.g. a joint venture) with respect to the relevant *cash centre*; and
- regulators such as the Financial Conduct Authority, the Payment Systems Regulator, and the Prudential Regulation Authority.

The Bank expects that the description provided by the *operator*, will include the name and other identifying details in respect of the stakeholder, and a description of the stakeholder's relationship to the *operator* (e.g. *wholesale customer* or *third-party provider*).

Communication strategy

Paragraph 1.3(9) of the *code of practice* requires *operators* to provide the Bank with information about the *operator's* communication strategy for the *cash centre closure*. The Bank expects that this will comprise a strategy for managing the dissemination of information in a timely and appropriate manner to stakeholders during the timeframe for implementation of the *cash centre closure*.

Governance

Paragraph 1.3(10) requires *operators* to include the job title and a description of the responsibilities of each individual designated as having responsibility for and being accountable to the *governing body* of the *operator* for oversight of the implementation, production, review and sign off of the *cash centre closure*.

The Bank expects that *operators* will have appropriately qualified and experienced individuals overseeing the proposal for *cash centre closure*, and that appropriate reporting to, and oversight by, an appropriately qualified and experienced management body, is in place.

Notification of proposed market exit

Paragraph 2.1 requires *recognised persons* to notify the Bank of their intention to cease performing a *specified relevant function* other than where the proposal is for a *cash centre closure*.

Paragraph 2.1 applies to an intention to cease performing all or part of a *specified relevant function*.

Recognised persons must notify the Bank of their intention to *exit*, at the earliest opportunity, and not less than twelve months in advance of the date on which the proposal is intended to take place.

Notification to the Bank must include certain information, including an assessment of the impact of the proposed *exit* on the ability of the *recognised person* to perform its *specified relevant functions*.

The guidance provided above in the context of notifications of *cash centre closures*, applies equally to the notification requirements for a *recognised person* in relation to a proposal to *exit* where relevant.

Notifications – additional requirements

Paragraph 3 requires a *recognised person* to keep the Bank up to date on the progress of a proposal for *cash centre closure* and *exit*. The Bank requires *recognised persons* to engage with the Bank in an open and co-operative manner and expects *recognised persons* to keep the Bank informed of material developments in, and changes to, the proposal.

Review period

Under paragraph 4.1 of the *code of practice*, unless otherwise required by any applicable law, regulation or rule, *recognised persons* must not take any irrevocable step towards a *cash centre closure* or *exit* before notifying the Bank in accordance with the *code of practice* and before the expiry of the relevant review period set out in paragraph 4.2.

The Bank considers that *recognised persons* may take steps, including disclosing a proposal for *cash centre closure* or *exit* to their employees, trade unions, shareholders, contracting parties and other stakeholders, where required to do so by an applicable law, rule or regulation. For example, where a *recognised person* is a listed company and considers that a market disclosure obligation will apply in respect of the proposal, then they may make that disclosure during the relevant review period.

However *recognised persons* should not serve a notice of termination of contract relating to a *cash centre closure* or *exit*, before the Bank has notified the *recognised person* that it has no objection to the proposed *cash centre closure* or *exit, or* until the expiry of the relevant review period, if earlier. Where the notice period for termination of a contract exceeds the relevant review period, *recognised persons* should notify the Bank of the proposed *cash centre closure* or *exit*, in sufficient time prior to the proposed date of notice of termination, to allow the Bank to consider the proposal.

Recognised persons are encouraged not to take any steps towards a *cash centre closure* or *exit* until the expiry of the relevant review period or, if earlier, the Bank has notified the *recognised person* that it has no objection to the proposal.