BANK OF ENGLAND

THE SCOTTISH AND NORTHERN IRELAND BANKNOTE RULES 2011

and

STATEMENT OF PENALTY POLICY

(These Rules are effective from 24 June 2011 and the Statement of Penalty Policy applies in respect of breaches from 11 May 2012.)

INTRODUCTION

Enabling provisions etc *4*

RULE 1 ..... **5**

CITATION, COMMENCEMENT, INTERPRETATION AND CONDITIONS **5**

Citation and Commencement *5*
Interpretation *5*
Elected business days *5*
Notices *6*
Conditions *6*

RULE 2 ..... **7**

VALUE OF BACKING ASSETS TO BE HELD **7**

Notes With the Potential to Enter Circulation *7*
Notes In Circulation *8*

RULE 3 ..... **10**

BACKING ASSETS **10**

Notes and Coin at Approved Locations *10*

RULE 4 ..... **13**

HOLDING OF BACKING ASSETS **13**

Specified Backing Assets *13*
Movement of Backing Assets *13*
Account at the Bank of England *14*
Notes at the Bank of England *14*

RULE 5 ..... **16**

EXCLUDED NOTES AND DESTRUCTION OF NOTES **16**

Excluded Notes *16*
Applications for Designation of Locations *17*
Movement of Excluded Notes *18*
Destruction of Notes *18*

RULE 6 ..... **21**

AGENTS **21**

RULE 7 ..... **23**

REPORTING AND PROVISION OF INFORMATION **23**

Reporting Deadlines *23*
Records *25*
Provision of Information *25*
Other Reporting Requirements *26*
Reporting Print Orders and Printing *26*
Annual Reports *27*
Report by a Skilled Person *27*
New Denominations *28*
Authorised Signatures *28*
Alternative Processing Procedures *28*

RULE 8 ..... **30**

REPORTING SYSTEM **30**

General Technical Requirements *30*
User Management *30*
Personnel *31*
Unlock Approved Data *31*
Static Data Changes *32*

RULE 9 ..... **33**

CONTINGENCY PLANS 33
RULE 10 34
CESSATION OF NOTE ISSUE 34
Notification *34*
Public Announcement *34*
Loss of Issuing Rights of the Authorised Bank *35*
Following Cessation *36*
RULE 11 37
NOTE EXCHANGE PROGRAMME 37
Specifications *37*
Loss of Issuing Right of Another Authorised Bank *38*
RULE 12 39
APPEALS RELATING TO PENALTIES 39
SCHEDULE 41
NIPS CODE OF CONNECTION 41
STATEMENT OF PENALTY POLICY 68
PENALTIES ..... ERROR! BOOKMARK NOT DEFINED.
Penalties *69*
Factors which the Bank may take into Account ..... *Error! Bookmark not defined.*

INTRODUCTION

Enabling provisions etc

1 The following Rules are made under Part 6 of the Banking Act 2009 (c. 1) and the Scottish and Northern Ireland Banknote Regulations 2009 (S.I. 2009/3056).

2 By virtue of section 11 of the Interpretation Act 1978 (c. 30), expressions used in Part 6 of that Act or in those Regulations have, unless the contrary intention appears, the same meaning in the Rules.

3 The Background and Commentaries do not form part of the Rules and have no legal effect.

RULE 1

Citation, Commencement, Interpretation and Conditions

Citation and Commencement

1.1 These Rules:

a. are made on 21 June 2011;
b. shall come into effect on 24 June 2011 and
c. may be cited as the Scottish and Northern Ireland Banknote Rules 2011.

1.2 The Scottish and Northern Ireland Banknote Rules 2010 are revoked.

Interpretation

1.3 In these Rules:

"accounting reference date" has the meaning given in section 391 of the Companies Act 2006 (c. 46);
"authorised signatures list" has the meaning given in Rule 7.36;
"the Bank" means the Bank of England;
"the Bank's appointee" means an officer or servant of the Bank or such other person as the Bank may appoint for the purposes of these Rules;
"business day" means a day other than:

(a) a Saturday or Sunday;
(b) Christmas Day or Good Friday; or
(c) a day which, in England and Wales, is a bank holiday under the Banking and Financial Dealings Act 1971 (c. 80); or
(d) subject to rule 1.4 (elected business days), a day which, in the relevant authorised bank's territory of issue is a bank holiday under that Act;

"Deposit Forecast" has the meaning given in Rule 2.6;
"Excluded Notes" means notes excluded from the backing assets requirements by virtue of Rule 5;
"financial year" has the meaning given in section 390 of the Companies Act 2006;
"note" means a banknote within the meaning of section 208 of the Act;
"specimen" has the meaning given in Rule 5.4;
"retained note" has the meaning given in Rule 5.4;
"the Notes IT System" means the Bank's information technology system for reporting data and for certain other matters under these Rules;
"the Regulations" means the Scottish and Northern Ireland Banknote Regulations 2009 and "regulation" is to be construed accordingly;
"value" means the face value of the notes or coin.

Elected business days

1.4 An authorised bank may, by notice to the Bank, elect to treat as a business day any day which under the Banking and Financial Dealings Act 1971 is a

bank holiday in its territory of issue and which is not a bank holiday in England and Wales.

1.5 Where an authorised bank makes an election under rule 1.4, that day is a business day for the purposes of the application of the Rules to that authorised bank until such time as the authorised bank gives notice to cancel the election.

Notices

1.6 All applications made and notifications given under these Rules must be in writing.

Conditions

1.7 Where the Bank imposes conditions relating to approved locations, Excluded Notes or Authorised Agents, an authorised bank must not disclose conditions imposed by the Bank, except:

a. where the Bank has given written consent to the disclosure; or
b. to the extent required by law; or
c. so long as the disclosure is in circumstances where a duty of confidentiality applies and the disclosure is only:
    i. to the extent required to give effect to those conditions;
    ii. to another authorised bank; or
    iii. to a legal or professional advisor.

Commentary

i A copy of the Rules will be sent to each authorised bank each time that they are changed.

ii The current Rules will be published on the Bank's website, www.bankofengland.co.uk.

iii Conditions may contain restricted information such as security or commercially sensitive information. Restrictions therefore apply to their disclosure.

RULE 2

Value of Backing Assets to be Held

Background

Rule 2 contains provisions about the calculation of "Notes With the Potential to Enter Circulation" and "Notes In Circulation", which are relevant to the calculation of backing assets and, under regulation 6(5), to the form in which backing assets must be held.

In setting the value of backing assets that must be held, the Bank may specify certain notes as Excluded Notes: such notes do not need to be backed. The requirements under which notes are to be excluded are contained in Rule 5, subject to such conditions as the Bank may impose.

The Banking Act 2009

Section 217 – Backing assets

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 6 – Backing assets

Regulation 7 – Value of backing assets to be held by an authorised bank

2.1 An authorised bank must hold backing assets to the value of all its notes, whether issued or not, except Excluded Notes.

2.2 Notes that must be backed fall into two categories: Notes In Circulation, and Notes With the Potential to Enter Circulation. For the purposes of these Rules, these must be calculated according to the following provisions.

2.3 Once a note being printed satisfies the definition of "banknote" in section 208 of the Act, it is a Note in Circulation unless:

a. the print location is a designated location for the purposes of Rule 5 and the requirements of that Rule and any relevant conditions are satisfied (in which case the note is an Excluded Note); or
b. the person contracted to print the notes is an Approved Agent under Rule 6, but the print location is not designated (in which case the note can be treated as a Note With the Potential to Enter Circulation).

Notes With the Potential to Enter Circulation

2.4 A Note With the Potential to Enter Circulation is a note of an authorised bank which it holds and which is not an Excluded Note.

2.5 An authorised bank may treat its notes held by an Approved Agent not as bearer as Notes With the Potential to Enter Circulation, provided that the authorised bank has not received any value in respect of those notes.

2.6 An authorised bank may treat as Notes With the Potential to Enter Circulation notes that it has received within a deposit of mixed notes which have been processed through a note counting machine to verify authenticity and value, but which have not yet been sorted from the other notes in the deposit (the 'Deposit Forecast').

2.7 In order to estimate the Deposit Forecast for the purposes of Rule 2.6, an authorised bank must use the following formula:

Total Value of the deposit * Y/Z, where:

Y = Value of the authorised bank's Notes In Circulation (in Scotland or Northern Ireland, as the case may be) as last reported, in £ millions.

Z = Value of total of all authorised banks' Notes In Circulation (in Scotland or Northern Ireland, as the case may be) as provided by the Bank, in £ millions.

Notes In Circulation

2.8 A Note In Circulation is a note of an authorised bank which is not a Note With the Potential to Enter Circulation or an Excluded Note.

2.9 An authorised bank must use the following formula to determine the value of its Notes In Circulation ("**NIC**") as at the commencement of Part 6 of the Act:

NIC = P - D - N - E

P is the value of all its notes ever printed.
D is the value of all its notes ever destroyed by the authorised bank or on its behalf.
N is the value of its Notes With the Potential to Enter Circulation (as calculated for the purposes of these Rules).
E is the value of its Excluded Notes (as calculated for the purposes of these Rules).

2.10 Thereafter, Notes in Circulation must be calculated as follows:

$$\mathbf{NIC_n = NIC_{(n-1)} + P_n - D_n +/- N_n +/- E_n}$$

$\mathbf{NIC_{(n-1)}}$ is the value of the **NIC** at the end of the previous period.
$\mathbf{P_n}$ is the value of notes printed during the period of calculation.
$\mathbf{D_n}$ is the value of notes destroyed during that period.
$\mathbf{N_n}$ is the value of the change in Notes With the Potential to Enter Circulation during that period (decrease to be added/increase to be deducted).
$\mathbf{E_n}$ is the value of the change in other Excluded Notes during that period (decrease to be added/increase to be deducted).

Commentary

i "Banknote" is defined in section 208 of the Act. For the purposes of these Rules, this first applies once the "promise to pay" and signature are added to a note.

ii Every note of an authorised bank ever produced and which has not been destroyed by or on behalf of the authorised bank is a 'Note in Circulation', a 'Note With the Potential to Enter Circulation', or an 'Excluded Note'. It follows

that notes of an authorised bank that, unknown to the authorised bank, have been accidentally destroyed while in circulation and so cannot be presented for payment, continue to count as Notes In Circulation for the purposes of Rule 2.

iii In normal circumstances, the authorised bank receives face value whenever one of its notes is put into circulation, by the person taking it as bearer. But notes which have been stolen from the authorised bank and not recovered are also in circulation, because face value is payable on demand on presentation by the bearer for payment.

iv The following is an example of a calculation of the Deposit Forecast for the purposes of calculating Notes With the Potential to Enter Circulation.

Where an authorised bank in Scotland has a deposit on a particular day of £1,060,000, its Notes In Circulation as last reported are £1,201 million and the figure for the total notes of authorised banks in Scotland in circulation as last provided by the Bank is £3,232 million, then:

*£1,060,000 * £1,201 million/£3,232 million = £393,892 of the deposited notes can be treated as the Deposit Forecast for the purpose of Notes With the Potential to Enter Circulation.*

RULE 3

Backing Assets

Background

Backing assets are assets used to back the note issue of an authorised bank.

The Regulations specify that at least 60% of an authorised bank's Notes In Circulation must be backed by Bank of England notes and UK coin and that the remainder, plus all Notes With the Potential to Enter Circulation, must be backed either by such notes and coin or by way of an interest bearing account at the Bank. Backing assets in the form of notes have to be held at the Bank or at a location approved for this purpose by the Bank, while backing assets in the form of coin must be held at a location approved for this purpose by the Bank (see Rule 4).

The Banking Act 2009

Section 217 – Backing assets

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 3 – Rules

Regulation 6 – Backing assets

Regulation 7 – Value of backing assets to be held by an authorised bank

Notes and Coin at Approved Locations

3.1 An authorised bank may only apply for a location to be approved by the Bank of England for the holding of its backing assets (an "approved location") if the location is within the United Kingdom.

3.2 An application by an authorised bank for the Bank to approve a location for the holding of its backing assets must include the following information:

a. full address of the property;
b. legal and beneficial owner of the property;
c. freehold/leasehold status of the property;
d. mortgages, liens and any other charges against the property;
e. details of all other persons with a legal or beneficial interest in the property;
f. OS 1:1250 scale map of the location marked with the boundaries of the property;
g. floor plan of the buildings forming part of the location;
h. details of insurance policy of the location including the risk covered, any excess and any limits;
i. any further information that the Bank may reasonably require.

3.3 If facilities at the location are to be operated on behalf of the authorised bank by a third party, the following information must also be provided:

a. legal name of the third party;
b. a copy of an outsourcing agreement in writing between the authorised bank and the third party;
c. any further information that the Bank may reasonably require.

3.4 Where the Bank has refused to grant an authorised bank approval of a location for the holding of its backing assets, any subsequent application by

the authorised bank in respect of that location must include details of any steps taken to remedy any deficiencies previously identified by the Bank and capable of remedy.

3.5 An authorised bank applying for the approval of a location for the holding of its backing assets must arrange for any inspections of the location by the Bank's appointee necessary or desirable to establish whether it is appropriate to grant approval.

3.6 Where the Bank grants an authorised bank approval of a location for the holding of its backing assets subject to conditions, the authorised bank must ensure that the approved location meets those conditions.

3.7 The Bank may revoke its approval of an approved location on such notice as is reasonable in the circumstances.

3.8 An authorised bank must permit the Bank's appointee to inspect its approved locations, or ensure that he or she can do so, for the purpose of monitoring continued compliance with the relevant Regulations, Rules and Conditions. Such inspections may take place unannounced and may include the opening of cages, parcels or packets of notes and bags or rolls of coin.

Commentary

Approved Locations

i Locations approved by the Bank for the holding of backing assets are referred to as 'approved locations'. They may (but need not) also be designated locations for the purposes of Rule 5.

ii The Bank will endeavour to notify the authorised bank of its decision regarding the approval of a location within sixty working days of the completed application being received. Where the approval process cannot be completed within sixty working days the Bank will inform the authorised bank of the reasons for the delay and the expected date by which a decision will be notified.

iii Approval of a location for the holding of backing assets will be confirmed to the authorised bank in writing, stating the date from which approval takes effect.

iv Where it grants approval, the Bank may impose conditions.

v Inspection by the Bank's appointee will normally be followed by a formal process of written feedback and a timetable for rectifying any problems identified, including provision for re-inspection where necessary or desirable.

vi The Bank may, at its own discretion, grant a location approval on a temporary basis until such time as the formal approval process can be completed. Such approval of any location does not necessarily mean approval will continue to be granted once the process is complete.

vii Approval may also be granted subject to conditions that the authorised bank must rectify any problems identified by the Bank within a certain timeframe.

viii The Bank may tailor the conditions to the characteristics of individual locations.

ix Where the Bank declines an application for approval, the Bank will provide a written explanation of the reasons for its decision and, where appropriate, the action that the Bank considers may be necessary for the location to be suitable

for approval.

- *The extent of notice for the revocation of the approved status of a location will depend on the circumstances of the case, including the seriousness of any breach of the relevant requirements or conditions. In some cases it may be necessary to revoke approval on the day that the authorised bank is notified. Once approval of a location is revoked, an authorised bank would be in breach of regulation 6(3) to hold note or coin there as backing assets.*

RULE 4

Holding of Backing Assets

Background

The Regulations provide that (except for notes held at the Bank) notes and coin held as backing assets must be held at a location approved by the Bank.

This Rule 4 specifies the denominations and series of notes that can be held as backing assets. The Rule also covers the holding of notes at the Bank as backing assets and some requirements for the interest bearing designated backing account.

The Banking Act 2009

Section 217 – Backing assets

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 6 – Backing assets

Regulation 7 – Value of backing assets to be held by an authorised bank

Regulation 8 – Interest on a designated account

Specified Backing Assets

4.1 The specified denominations and series of Bank of England notes for the purpose of Regulation 6(2)(a)(backing assets) are:

a. where the note is held by the Bank for the purpose of regulation 6(3)(a), any series and any denomination of note;
b. where the note is held at an approved location in accordance with regulation 6(3)(b):
    i. the series from time to time being issued by the Bank of any denomination which is legal tender in England and Wales under section 1 of the Currency and Bank Notes Act 1954 (c. 12); and
    ii. any denominations of series E or series F, including any variants of those series.

Movement of Backing Assets

4.2 Industry standard vehicles of members of the British Security Industry Association (BSIA) are approved locations for the purpose of transporting backing assets between the (non-vehicular) approved locations of any authorised bank, subject to the following conditions:

a. the notes or coin must be insured for full value whilst in transit between such locations;
b. the notes or coin must not be in a vehicle for longer than 48 hours before being delivered to a (non-vehicular) approved location;
c. the vehicle must remain within the United Kingdom; and
d. the notes or coin must be reported as specified in Rule 4.3 and Rule 7.

4.3 Where an authorised bank intends to move backing assets in accordance with Rule 4.2 between 4pm on a day and 6am on the following day:

a. in the report it gives as of 4pm, it must report those backing assets as in transit during that period; and
b. if the backing assets are delivered to a (non-vehicular) approved location of the authorised bank during that period, it must hold them as backing assets under the appropriate conditions at that location until 6am the next business day.

4.4 Where an authorised bank reports backing assets as held at one of its (non-vehicular) approved locations in the report it gives as of 4pm on a day, it must hold those backing assets as backing assets at that approved location until 6am the next business day.

Account at the Bank of England

4.5 An application by the authorised bank for the Bank to open a sterling account in the name of the authorised bank and to designate it as a backing account (a "designated backing account") must include a copy of the Bank's designated backing account Terms and Conditions, as provided by the Bank, signed on behalf of the authorised bank.

4.6 The authorised bank may only make a request to withdraw funds from its designated backing account:

a. where permitted by the Bank, through the Notes IT System portal in accordance with the Bank's procedures; or
b. in the event that the authorised bank cannot use the portal (whether because it lacks permission or because the portal is unavailable), using the Alternative Processing Procedures specified in Rule 7.

4.7 An authorised bank must give the Bank at least three working days notice of any request to change the account into which payment may be made from its designated backing account.

4.8 An authorised bank may not withdraw funds from its designated backing account where the Bank has notified it that the Bank is of the opinion that a withdrawal would result in the authorised bank failing fully to back its note issue.

4.9 Any interest on a designated backing account shall be credited to the account at the end of each month so as to be available on the first day of the following month which is a business day for the Bank.

Notes at the Bank of England

4.10 An authorised bank may only hold backing assets in the form of notes at the Bank if it has a designated backing account.

4.11 Where an authorised bank holds backing assets in the form of notes at the Bank, the value of the notes must be a multiple of £5.

4.12 An authorised bank wishing to acquire notes from the Bank to be held at the Bank as backing assets or return such notes to the Bank must:

a. make the relevant request on a day which is a business day for the Bank, by 2pm on the day in question;
b. instruct the Bank to fund the transaction by debiting or (as the case may be) crediting its designated backing account; and
c. where permitted by the Bank, use the Notes IT system portal in accordance with the Bank's procedures; or
d. in the event that the authorised bank cannot use the portal (whether because it lacks permission or because the portal is unavailable) make requests using the Alternative Processing Procedures specified in Rule 7.

Commentary

Movement of Backing Assets

i Notes or coin reported as backing assets can be transferred between an authorised bank's approved locations without ceasing to be backing assets.

ii The expectation is that under normal circumstances notes or coin in transit will be delivered to a non-vehicular location within 24 hours. However, Rule 4.2 provides a 48 hour limit.

iii Apart from the period between 4pm on a business day and 6am on the following business day, these Rules do not preclude an authorised bank from replacing backing assets with other backing assets, provided that the replacement backing assets are in place and satisfy all the relevant requirements and conditions before the original backing assets are removed.

iv If the conditions for the Approved Location at which the backing assets are being held are breached (for example, as a result of a successful robbery) then steps must be taken immediately to ensure that any notes and/or coins that have ceased to be backing assets are replaced at the earliest possible opportunity.

Account at the Bank of England

v The interest bearing account at the Bank of England for holding backing assets is known as the 'designated backing account'.

vi The designated backing account is also to be used in relation to the funding of any acquisitions by the authorised bank of notes to be held as backing assets at the Bank of England.

vii In the event of the Notes IT system being unavailable the Alternative Processing Procedures contained in Rule 7 are to be used.

RULE 5

Excluded Notes and Destruction of Notes

Background

"Excluded Notes" do not have to be backed provided that the relevant requirements of this Rule 5 and any conditions specified by the Bank are satisfied.

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 7 – Value of backing assets to be held by an authorised bank

Excluded Notes

5.1 Notes of an authorised bank are Excluded Notes provided that:

a. they are held at a location designated in accordance with this Rule 5 (a "designated location");
b. all conditions which the Bank specifies as applicable to the notes are complied with; and
c. the notes are:
    i. new notes;
    ii. notes awaiting destruction;
    iii. notes held by the printer;
    iv. returned notes; or
    v. working stock.

5.2 Notes of an authorised bank which are not in a category included in Rule 5.1 are Excluded Notes provided that:

a. they are held at a location designated in accordance with this Rule 5 (a "designated location");
b. they are reported as "retained notes" for the purposes of Rule 7.25;
c. the authorised bank or its Approved Agent maintains an up to date record of the value of notes held as retained notes and is able to supply this record to the Bank on request;
d. no more than £100,000 is held as retained notes;
e. the retained notes are stored securely when not in use, although they need not be stored in a cage or a vault; and
f. a process is in place to report to the Bank details of the destruction of these notes.

5.3 Notes which are not in a category specified in Rule 5.1 or 5.2 are Excluded Notes if:

a. the Bank has specified conditions for the purpose of this Rule 5.3; and
b. those conditions are complied with.

5.4 For the purposes of this Rule 5:

- "bulk destruction" means destruction of notes by a separate process of granulation/shredding following completion of the sorting process;
- "new notes" means uncirculated notes of an authorised bank held in unopened parcels, as packed by the printer (as defined below);
- "notes awaiting destruction" means notes of an authorised bank awaiting destruction, having been deemed by the authorised bank as unfit to return to circulation, or being of a design that the authorised bank is no longer issuing;

- "notes held by the printer" means notes which are held by the printer (as defined below) in that capacity and which satisfy the definition of "banknote" in section 208 of the Act, including spoilage but not including notes which have completed all stages of the printing process;
- "on line destruction" means destruction of notes by a note sorting machine as part of the sorting process;
- "retained notes" means notes which do not satisfy the definition of a specimen (as defined below) but are retained at the completion of a print run for the purposes of use as master machine proofs, laboratory testing sheets and colour sheets and which (although of a design which could circulate as money) are not intended for circulation;
- "returned notes" means notes of an authorised bank that have been returned to the authorised bank after being processed through a note sorting machine by another commercial issuer, to verify authenticity and confirm value, and for which value has been given;
- "specimen" means notes of an authorised bank which have been stamped with the word "specimen", or have been hole punched, and are not intended for circulation;
- "the printer" means a person contracted by the authorised bank to print the notes; and
- "working stock" means notes of an authorised bank that have previously been issued, are not issued, but are being held by the authorised bank awaiting reissue.

Applications for Designation of Locations

5.5 An authorised bank may only apply for the Bank to designate a location for the holding of its Excluded Notes if the location is within the United Kingdom.

5.6 Any application by an authorised bank for the Bank to designate a location must include the following information:

a. full address of the property;
b. legal and beneficial owner of the property;
c. freehold/leasehold status of the property;
d. mortgages, liens and any other charges against the property;
e. details of all other persons with a legal or beneficial interest in the property;
f. OS 1:1250 scale map of the location marked with the boundaries of the property;
g. floor plan of the buildings forming part of the location;
h. details of insurance policy of the location including the risk covered, any excess and any limits;
i. any further information as the Bank may reasonably require.

5.7 If the facilities at the location are operated on behalf of the authorised bank by a third party, the following information must also be provided:

a. legal name of the third party;
b. a copy of an outsourcing agreement in writing between the authorised bank and the third party;
c. any further information that the Bank may reasonably require.

5.8 Where the Bank has refused to designate a location, any subsequent application by the authorised bank in respect of that location must include

details of steps taken to remedy any deficiencies identified by the Bank and capable of remedy.

5.9 An authorised bank applying for designation of a location must arrange for any inspections of the location by a Bank's appointee necessary or desirable to establish whether it is appropriate to designate the location.

5.10 The Bank may revoke its designation of a location on such notice as is reasonable in the circumstances.

5.11 An authorised bank must permit the Bank's appointee to inspect its designated locations, or ensure that he or she can do so, for the purpose of monitoring continued compliance with the Regulations, Rules and Conditions. Such inspections may take place unannounced and may include the opening of cages, parcels or packets of notes.

Movement of Excluded Notes

5.12 Industry standard vehicles of members of the British Security Industry Association (BSIA) are designated locations for the purpose of transporting notes between the (non-vehicular) designated locations of any authorised bank, subject to the following conditions:

a. the notes must be insured for full value whilst in transit between such locations;
b. notes must not be in a vehicle for longer than 48 hours before being delivered to a (non-vehicular) designated location; and
c. the notes must be reported as specified in Rule 5.13 and Rule 7.

5.13 Where an authorised bank intends to move Excluded Notes in accordance with Rule 5.12 between 4pm on a day and 6am on the following business day:

a. in the report it gives as of 4pm, it must report those Excluded Notes as in transit during that period; and
b. where the Excluded Notes are delivered to a (non-vehicular) designated location of the authorised bank during that period, it must hold them as Excluded Notes at that location until 6am the next business day under the appropriate conditions.

5.14 Where an authorised bank reports certain Excluded Notes as held at a (non-vehicular) designated location in the report it gives under Rule 7 as of 4pm on a day, it must continue to hold those notes as Excluded Notes at that designated location until 6am the next business day.

Destruction of Notes

5.15 When an authorised bank destroys its notes, it must ensure that they are granulated or shredded using appropriate machinery so as to make it impossible to reconstruct an individual banknote.

5.16 Bulk destruction may take place at the authorised bank's own premises or elsewhere.

5.17 An authorised bank must, within one month of a request by the Bank, provide the Bank with such certificates for on-line destruction as the Bank may from time to time require.

5.18 An authorised bank must retain records relating to on-line destruction for a period of no less than two years from the date of destruction taking place.

5.19 If the note destruction machinery breaks down during the destruction process, so as to prevent an authorised bank from completing the destruction in time for the reporting deadline, the authorised bank must:

a. before the relevant reporting deadline, notify the Bank that there has been such a breakdown;
b. confirm to the Bank its best estimate of the values of notes destroyed and notes not yet destroyed;
c. ensure that the notes which were due for destruction but are not yet destroyed are held as Excluded Notes (save that packing requirements do not apply);
d. retain CCTV footage of the event until further notice.

5.20 For the purposes of reporting under Rule 7:

a. for any report due within 24 hours of the breakdown, the authorised bank may report based on figures calculated as if no notes have been destroyed as part of the process;

b. for any report due more than 24 hours after the breakdown, the authorised bank must count the notes which were due for destruction but are not yet destroyed and report on the actual value of notes not yet destroyed.

Commentary

Excluded Notes

i. Locations approved by the Bank for the holding of certain categories of Excluded Notes are referred to as 'designated locations'. They may (but need not) also be approved locations for the purposes of Rule 3.

ii. The categories of notes in Rule 5.1 are treated as Notes With the Potential to Enter Circulation if they are not held at a designated location in accordance with the relevant requirements and conditions.

iii. Notes held by the printer, i.e. those which have not concluded all stages of the print process are Excluded Notes if the print location is a designated location and the notes are stored appropriately. Such notes could be, for example, notes in uncut sheets or notes which are produced as part of the printing process but which will be destroyed at the end of that process.

iv. Notes are not considered to have completed the printing process until they have been packaged.

v. Notes held in the vault at the printer prior to being issued for the first time should be reported as 'new notes', while notes in the print hall or waste storage room should be reported as 'notes held by the printer'.

vi. The Bank will endeavour to notify the authorised bank of its decision regarding the approval of a designated location within sixty working days of the completed application being received. Where the approval process cannot be completed within sixty working days the Bank will inform the authorised bank in writing of the reasons for the delay and the expected date by which a decision will be

notified.

vii. *Designation of a location will be confirmed to the authorised bank in writing, stating the date from which designation takes effect.*

viii. *The Bank may impose conditions where it designates a location.*

ix. *Inspection by the Bank's appointee will normally be followed by a formal process of written feedback and a timetable for rectifying any problems identified, including provision for re-inspection where necessary or desirable.*

x. *The Bank may, at its discretion, grant designation of a location on a temporary basis until such time as the formal approval process can be completed. Such designation of any location does not necessarily mean approval will continue to be granted once the process is complete.*

xi. *Designation of a location may also be granted subject to conditions that the authorised bank must rectify any problems identified by the Bank within a certain timeframe.*

xii. *Where the Bank declines an application for designation, the Bank will provide a written explanation of the reasons for its decision and, where appropriate, the necessary corrective action.*

xiii. *The Bank may tailor the conditions to the characteristics of individual locations.*

xiv. *The extent of notice for the revocation of the designation of a location will depend on the circumstances of the case, including the seriousness of any breach of the relevant requirements or conditions. In some cases it may be necessary to revoke designation on the day that the authorised bank is notified. Once designation of a location is revoked, any notes held there will need to be immediately backed.*

xv. *Apart from the period between 4pm on a business day and 6am on the following business day, these Rules do not preclude an authorised bank from removing Excluded Notes from the conditions for exclusion, provided that backing assets satisfying all the relevant requirements and conditions are in place to back the Excluded Notes before they are withdrawn.*

xvi. *If the conditions for the designated location at which the Excluded Notes are being held are nevertheless breached (for example, as a result of a successful robbery) then steps must be taken immediately to ensure that the notes that have ceased to be Excluded Notes are backed at the earliest possible opportunity.*

RULE 6

Agents

Background

The Bank may approve an agent of the authorised bank, such as another commercial bank, cash handler or printer of notes, to hold notes of the authorised bank not as bearer, and thereby enable those notes to be backed as Notes With the Potential to Enter Circulation. This Rule covers the requirements imposed on the authorised bank in this situation.

The Banking Act 2009

Section 218 – Information

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 10 – Unissued banknotes

6.1 An application by an authorised bank for a person to be approved to hold its notes other than as bearer (an "Approved Agent") must include the following information:

a. full legal name of the agent;
b. details of the usual business of the agent;
c. specific tasks the agent will carry out on behalf of the authorised bank;
d. location(s) where the authorised bank's notes, not being held as bearer, will be held by the agent;
e. details of the insurance policy of such location(s), including the risk covered, any excess and any limits;
f. any further information that the Bank may reasonably require.

6.2 An authorised bank must, in respect of each of its Approved Agents, ensure that the Approved Agent certifies (within five working days of the anniversary of approval) that any notes held by the Approved Agent in the past year as agent have not been held as bearer.

6.3 An authorised bank must, in respect of any Approved Agent that prints notes for it, ensure that the Approved Agent, within one month of any print order being completed, provides the Bank with certificates relating to the printing, specifying the exact series, denomination and number of notes printed for the issuing bank.

6.4 An authorised bank with an Approved Agent must authorise and instruct the agent to cooperate with the Bank in relation to any enquiry that the Bank makes to verify the value and denominations of the authorised bank's notes that the agent holds or has held other than as bearer.

6.5 It is a condition of an approval under Rule 6.1 that upon request by the Bank:

a. the authorised bank must provide a demonstration or explanation of the procedures that are in place for the Approved Agent to report to it when notes are issued by the agent;
b. the authorised bank must submit its records relating to notes held by an Approved Agent, other than as bearer, to the Bank for audit.

6.6 An authorised bank must, in respect of any Approved Agent that destroys notes for it, ensure that the Approved Agent:

a. provides the Bank with a destruction certificate for any bulk destruction carried out on behalf of the authorised bank within one month of the destruction being completed;
b. provide such certificates for on-line destruction as the Bank may from time to time require within one month of a request being made;
c. retains records relating to on-line destruction for a period of no less than two years from the date of destruction taking place.

Commentary

i. Notes held by an Approved Agent other than as bearer are Notes With the Potential to Enter Circulation. It is possible for an Approved Agent to hold notes as Excluded Notes provided that the notes are held at a designated location. Where an authorised bank wants this arrangement to apply, an application for the designation of the location where those notes will be held needs to be made under Rule 5.

ii. Notes held by an Approved Agent may only be Notes With the Potential to Enter Circulation if they are held not as bearer. Whenever an agent acquires notes of an authorised bank for value, those notes are Notes In Circulation and the agent is the bearer.

iii. In practice the Bank would usually expect Approved Agents to be persons such as financial institutions and/or professional cash handlers with adequate control procedures and experience in cash processing/distribution. A printer could also be an Approved Agent.

iv. Where the Bank deems it necessary the Bank may withdraw approval of the agent.

RULE 7

Reporting and Provision of Information

Background

Authorised banks are required to report data to the Bank. Some data can be reported for a preceding period, but some must be reported on a same day basis. The data that are required to be reported daily are needed for compliance purposes, as without this information the Bank cannot effectively ensure that the backing requirements are being complied with at all times. In addition to the data reporting, the Act and Regulations make provision for annual reports and reports by skilled persons.

The Banking Act 2009

Section 218 – Information

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 13 – Provision of information to the Bank of England

Regulation 14 – Reports as to banknotes and backing assets

Regulation 15 – Independent reports

Reporting Deadlines

7.1 An authorised bank must report to the Bank in respect of the notes listed in column 1 of Table 1 at the frequency in column 2 by the deadline in column 3 in accordance with Rules 7.2 to 7.14.

Column 1 **Data to be Reported**	**Column 2** **Reporting Frequency**	**Column 3** **Reporting Deadline (subject to rule 7.4)**
Excluded Notes: value by denomination held, by each category of Excluded Note, at each designated location (as applicable) as at 4pm on the day.	Report for every day (including non-business days).	4.30pm on each day.
Backing assets held in the form of notes: value by denomination held at each approved location as at 4pm on the day.	Report for every day (including non-business days).	4.30pm on each day.
Backing assets held in the form of coin: total value held at each approved location as at 4pm on the day.	Report for every day (including non-business days).	4.30pm on each day.
Notes In Circulation: total	Report for every day (including non-business	5pm on each Thursday in respect of each day of the

value	days).	preceding week.
Notes With the Potential to Enter Circulation: total value.	Report for every day (including non-business days).	5pm on each Thursday in respect of the days of the preceding week.
Destruction of notes: value by denomination.	Report for each day of the preceding week (including non-business days) on which destruction took place.	5pm on each Thursday.

7.2 A reporting week runs from midnight at the start of Thursday to midnight at the end of the following Wednesday.

7.3 The authorised bank must report its data by using the Notes IT System in accordance with Rule 8 or such other reporting system as the Bank may require.

7.4 Where an authorised bank does not intend to make a report on a non-business day:

a. it must report information required on a daily basis by 4.30pm on the preceding business day;
b. it may report information required on a weekly basis by 5pm on the next business day.

7.5 Before the deadline in column 3, a signatory listed on the authorised bank's authorised signatories list must approve the reporting data entered in the system.

7.6 If a signatory listed on the authorised bank's authorised signatories list does not approve the data entered into the reporting system before the deadline, the data is not considered to have been reported.

7.7 An authorised bank may report some or all of:

a. its Excluded Notes as Notes With the Potential to Enter Circulation or Notes in Circulation;
b. its Notes With the Potential to Enter Circulation as Notes in Circulation.

7.8 When an authorised bank calculates the value of Excluded Notes, Notes in Circulation and Notes With the Potential to Enter Circulation for its daily reporting, each of its notes must appear in only one of those categories on any given day.

7.9 The authorised bank must provide the Bank with a breakdown by denomination of Notes in Circulation and Notes with the Potential to Enter Circulation on a quarterly basis as at the first day of March, June, September and December and on an ad hoc basis at the Bank's request. This information should be e-mailed to the Bank within one week of the reporting date or request.

7.10 Where an authorised bank does not have historic data for the value of Notes In Circulation by denomination, it may report the value of notes for which denomination is unknown as 'denomination unknown'.

7.11 For reporting Notes With the Potential to Enter Circulation,:

a. the breakdown by denomination must be by:
    i. actual denomination; or
    ii. a reasonable estimate of the breakdown of denomination, provided that the authorised bank has first notified the Bank of its method of calculation;
b. the value for 'Deposit Forecast' may be entered without a breakdown by denomination;
c. the value of notes held in its branches, excluding notes held in ATMs, may be estimated, subject to Rule 7.13;
d. the value of notes held in ATMs may be estimated for non-business days, subject to Rule 7.14.

7.12 Where an authorised bank reports a value for 'Deposit Forecast' it must deduct this from the value of Notes in Circulation and, for this purpose, it may estimate the resulting change to the denominations of Notes in Circulation.

7.13 Where an authorised bank wishes to estimate the value of its notes held in its branches (excluding ATMs):

a. it must calculate the actual value of its notes held in its branches for at least one day per week and report the actual value for that day;
b. for any other day, it may report an estimate, which must be at least five percentage points lower than N * P where:
    i. **N** is the total actual value of all notes held in its branches for the day in question;
    ii. **P** is the average percentage of the authorised bank's own notes in its branches, calculated as the average figure over the preceding three months of the days for which actual values were obtained, compared to the actual total value of all notes held in its branches for each such day.

7.14 Where an authorised bank estimates the value of notes held in ATMs for the purpose of reports for non-business days, it must base its estimate on the change in the actual value from the report for the preceding business day to the report for the following business day, taking into account any additional funds loaded into the ATMs and distributing the change evenly over the period between the reports on the two business days.

Records

7.15 An authorised bank must ensure:

a. that at each of its approved locations a record is maintained of the denominational breakdown of backing assets held in the form of coin at that location.
b. where the location is managed by an Approved Agent, that the Approved Agent maintains such a record.

7.16 The authorised bank must provide to the Bank such of this information as the Bank may from time to time request.

Provision of Information

7.17 An authorised bank must provide such additional information as the Bank may from time to time require for the purpose of exercising its functions

under the Regulations or the Rules or verifying or monitoring an authorised bank's compliance with a provision of the Regulations, Rules or Conditions.

Other Reporting Requirements

7.18 An authorised bank must provide to the Bank such additional information on its notes held by Approved Agents other than as bearer as the Bank may from time to time require.

7.19 Where the authorised bank's banknote printing is not undertaken by an Approved Agent, the authorised bank must provide the Bank with certificates relating to the printing of notes within one month of the print order being completed. The certificate must specify the exact series, denomination and number of notes printed for the issuing bank.

7.20 Where an authorised bank undertakes its own bulk destruction of its banknotes, it must provide the Bank with a destruction certificate within one month of the destruction being completed.

7.21 An authorised bank must notify the Bank and provide it with full details without delay in the event that it becomes aware of any of the following circumstances having an impact on it in relation to its notes or backing assets, except where the matter relates to counterfeiting:

a. commencement of civil proceedings;
b. prosecution for an offence involving fraud or dishonesty;
c. any alleged acts of fraud;
d. reporting or recording irregularities, whether or not there is evidence of possible fraud;
e. any matter that could have a serious regulatory impact on the authorised bank, including affecting the authorised bank's reputation or ability to provide adequate service and protection to its noteholders.

7.22 An authorised bank must notify the Bank and provide it with relevant information without delay if any of the following circumstances occur:

a. a transaction or linked transactions results in a change in ownership of shares with aggregate voting rights of 30% or more in:
   i. the authorised bank; or
   ii. a parent undertaking of the authorised bank, within the meaning of section 1162 of the Companies Act 2006;
b. a change of legal or trading name of the authorised bank;
c. a change in the address of its registered office.

Reporting Print Orders and Printing

7.23 An authorised bank must, at least one month before the commencement of a print run, notify the Bank of the print order, providing details of the estimated date of completion and the values of each denomination to be printed.

7.24 During a print run, the authorised bank must report the total value of notes which have been printed, by denomination, on a daily basis.

7.25 An authorised bank must provide the Bank with a reconciliation of each print order for the printing of its notes:

a. within one month of the completion of a print order, associated verification checks in respect of the storage of specimens and retained notes and the destruction of any spoilage; and
b. containing sufficient information to enable the Bank to establish that the total of new notes, specimens, retained notes and spoilage destroyed equals the total value of notes which could have been printed from the declared opening notional value of paper used in the printing process.

Annual Reports

7.26 An authorised bank must, for each financial year, provide the Bank with a report prepared by a suitably qualified and experienced independent auditor appointed by the authorised bank (the "annual report").

7.27 The authorised bank must provide the annual report within three months of the relevant accounting reference date.

7.28 The auditor's report must:
a. state the scope of the auditor's work and any limitations that the auditor faced in completing its work or providing its opinion;
b. include a signed statement of the auditor's opinion as to the design and operational effectiveness of the authorised bank's control environment for reporting accurate and timely data to the Bank.

7.29 The scope of the auditor's work must include:
a. evaluation of controls over the collation, calculation, validation, input and approval of the data reported to the Bank,
b. evaluation of the compliance of the authorised bank with the Bank's NIPS Security Code of Connection;
c. evaluation of controls over the accuracy of data provided by Approved Agents and other third parties which is used to determine the figures reported to the Bank;
d. evaluation of any estimations and assumptions used to determine the figures reported to the Bank;
e. evaluation of procedures established by the authorised bank to ensure compliance at all times with the Regulations, Rules and Conditions;
f. validation of the accuracy of data reported to the Bank, using appropriate sampling techniques. The auditor's testing should cover the entire financial year and each of the following types of data:
i. Value of Notes In Circulation;
ii. Value of Notes With the Potential to Enter Circulation;
iii. Value by denomination of Excluded Notes held at designated locations;
iv. Value by denomination of backing assets held at approved locations.

7.30 The auditor's report may include such matters as the auditor considers relevant in addition to those specified in rule 7.29.

7.31 The costs associated with providing the annual report are to be borne by the authorised bank.

Report by a Skilled Person

7.32 An authorised bank must provide a report to the Bank prepared by a person nominated or approved by the Bank (a "nominated skilled person") where:

a. the Bank has notified the authorised bank that it has nominated or approved the person in accordance with regulation 15(3);
b. the notice confirms the matter about which the Bank requires a report; and
c. the notice specifies the period to which the report must relate.

7.33 In such circumstances, the authorised bank must:

a. appoint and instruct the nominated skilled person to prepare a report in accordance with the notice; and
b. provide the nominated skilled person with such access, assistance, information and explanations as the nominated skilled person requires in order to prepare the report.

7.34 The costs associated with providing a report by a nominated skilled person are to be borne by the authorised bank.

New Denominations

7.35 An authorised bank intending to issue a denomination of note other than £1, £5, £10, £20, £50 or £100 must notify the Bank at least six months before the new denomination is first issued.

Authorised Signatures

7.36 An authorised bank must provide the Bank with an authorised signatures list including a specimen signature of each person authorised by that bank to sign documents for the purposes of these Rules (an "authorised signatures list").

7.37 An authorised bank must notify the Bank of any changes to its authorised signatures list and, where appropriate, provide an updated authorised signatures list.

Alternative Processing Procedures

7.38 In the event that any of the standard processing or reporting systems is not available or the authorised bank is not permitted to use them, the following procedures must be used (and which may not be used if the standard systems are available and their use is permitted):

a. an authorised bank must complete such forms as the Bank may require;
b. all such forms must be signed by an authorised signatory and where required contain a valid random security number from a list of random security numbers provided to the authorised bank by the Bank;
c. deadlines for reporting using these procedures are the same as for standard procedures.

Commentary

i When estimates of the denominational split of Notes With the Potential to Enter Circulation or Notes In Circulation are reported, the total of the estimates should equal the total value of the authorised bank's Notes With the Potential

to Enter Circulation or Notes In Circulation in existence at that time.

ii Rule 7.7 ensures that the figures calculated for the value of Excluded Notes, Notes in Circulation and Notes With the Potential to Enter Circulation for its daily reporting will be the total of all the notes of the authorised bank, i.e. each note is included once and only once.

Reporting Print Orders and Printing

iii The value of Excluded Notes to be reported by the authorised bank on a daily basis should include the total value of notes which have completed the printing process on that day and which satisfy the definition of a banknote in section 208 of the Act.

***Alternative Processing Procedures**.*

iv Random security numbers and instructions for their use will be provided by the Bank to each authorised bank separately.

Auditors report

v The list of matters in rule 7.29 is not intended to be exhaustive. At the request of the authorised bank, the auditor's report may include additional matters and authorised banks are encouraged to use the auditor's work as an opportunity to test, in general, the robustness of their systems and controls".

RULE 8

Reporting System

Background

This Rule 8 relates to technical, procedural, policy, physical and personnel issues which could impact security in relation to the Bank's Notes IT System.

The Banking Act 2009

Section 218 – Information

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 14 – Reports as to banknotes and backing assets

8.1 Rule 8 concerns access to the Notes IT System by authorised banks for inputting data relating to Scottish and Northern Ireland banknotes.

General Technical Requirements

8.2 An authorised bank must provide and use PCs (whether desktop or laptop) to access the Notes IT System.

8.3 When connecting to the Bank's NIPS portal an authorised bank may use:
a. a corporate desktop computer or corporate managed laptop which is connected to the authorised bank's internal network; or
b. a corporate managed laptop, which has remote access to the authorised bank's internal network.

8.4 The authorised bank must comply with the NIPS Code of Connection (included as a Schedule to these Rules). Each year the authorised bank must complete an annual self-certification of compliance, as set out in Appendix B of the Code of Connection.

User Management

8.5 An authorised bank must ensure that:
a. only those of its staff which are confirmed by the Bank as users of the Notes IT Systems for the time being use the system;
b. each of its users of the Notes IT system has been security cleared by the authorised bank within the past five years; and
c. every such user complies with the Bank's Acceptable Usage Policy.

8.6 An authorised bank must:
a. ensure that all of its staff who access the Notes IT System sign an "Acceptable Usage Policy Form" provided by the Bank;
b. ensure the form is signed by at least two signatories in accordance with its authorised signatures list and includes a valid random security number from a list of random security numbers provided to the authorised bank by the Bank;

c. submit each completed form to Notes Accounting at the Bank by fax or secure e-mail.

8.7 Where an authorised bank wishes the Bank to add, amend, suspend or revoke a member of the authorised bank's staff as a user of the Notes IT System it must:
a. use an "S&NI – User Access Request form" provided by the Bank;
b. ensure that the application is signed by at least two signatories in accordance with its authorised signatures list and includes a valid random security number from a list of random security numbers provided to the authorised bank by the Bank; and
c. submit the application to Notes Accounting at the Bank by fax or secure e-mail.

Personnel

8.8 An authorised bank must inform the Bank at least three business days in advance of any staff member with access to the Notes IT System ceasing to work for the authorised bank, so as to allow for access to be revoked at the time of leaving.

8.9 An authorised bank must request the suspension of a member of its staff as a user of the Notes IT System:
a. within two business days, if disciplinary proceedings are commenced in relation to the member of staff, unless the disciplinary proceedings are for a matter with no security implications (for example, time-keeping or attendance);
b. if the member of staff is on an extended absence (such as maternity leave or long-term sick leave); or
c. if there is no current business need for the member of staff to have access.

Unlock Approved Data

8.10 Where an authorised bank requires approved data to be unlocked by the Bank, it must:
a. use a "Request to Unlock Data form", provided by the Bank;
b. include information on both the data to be amended and the revised data;
c. ensure the application is signed by at least two signatories in accordance with its authorised signatures list and includes a valid random security number from a list of random security numbers provided to the authorised bank by the Bank; and
d. submit the request to Notes Accounting at the Bank by fax or secure e-mail.

8.11 Where a "Request to Unlock Data form" which complies with the requirements set out in 8.10 is received before the reporting deadline (as per Rule 7.1), the revised data on the form are to be treated as the reported data.

8.12 Where, following a request under Rule 8.10 the Bank confirms that the requested data has been unlocked, the authorised bank must, within three business days:

a. make such changes to the data as may be required;
b. ensure that an authorised signatory approves the data; and
c. inform the Bank on completion.

Static Data Changes

8.13 A request by an authorised bank for the Bank to make a change to the parts of the recorded data in the Notes IT System which the Bank controls (such as drop down menus and categories) must be made in writing.

Commentary

i The security of systems and information used for the S&NI regime is of key importance to the Bank of England. Information Technology (IT) security concerns the appropriate preservation of confidentiality, integrity and availability of information and information processing activities that are supported as part of the S&NI regime.

ii The user will be required to provide authenticating details (a user name and password) before being given access to a system interface. They then will be required to re-provide authenticating details to the interface (user name and password) before being granted access to specific data and information. Users will be provided with a remote access token and a PIN that will be used for authentication to the Bank's remote access platform.

iii Any queries from users or requests for assistance must be made to the Notes Accounting Team, initially by telephone (020 7601 3351). Requests which are sensitive or could have security consequences (e.g. the resetting of passwords) may need to be confirmed by authenticated fax or other means.

iv Where the Bank receives a written request to change parts of the recorded data in the Notes IT System which the Bank controls (such as drop down menus and categories), if it considers that a change is appropriate, the Bank will endeavour to make these changes as soon as practicable.

RULE 9

Contingency Plans

Background

Events that could cause an authorised bank to fail, or a sudden increase in demand for notes from one or more issuer or the Bank, need to be managed and planned for to ensure both noteholder protection and that public confidence in notes is maintained.

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 3 – Rules

Regulation 26 – Rules relating to a note exchange programme and destruction of banknotes

9.1 An authorised bank must prepare and maintain a contingency plan.

9.2 The authorised bank must submit to the Bank a draft of the contingency plan annually on or before 1 July in each year or such other date as the Bank may agree.

9.3 The authorised bank must incorporate into the contingency plan such amendments to the draft as the Bank may reasonably require.

9.4 The authorised bank's contingency plan must cover, as a minimum, the following scenarios:

Scenario A: An event, which leads to a sudden, short-term, unanticipated increase in demand for notes being, for these purposes, an increase in demand of 20% or more over the typical value for that time of year of:

i. the notes of the authorised bank;
ii. the notes of another authorised bank;
iii. the notes of all authorised banks.

Scenario B: A theft of its notes to the value of 5% or more of its Notes In Circulation, resulting in the need urgently to withdraw one or more denominations.

Scenario C: The counterfeiting of one or more of its note designs so that it has to remove that design or those designs from circulation.

Scenario D: The loss of issuing rights by one or more other authorised banks which issue notes in the same territory as the authorised bank.

9.5 The authorised bank must include in its contingency plan detailed processes to be followed in each of the scenarios A to D.

9.6 The authorised bank must carry out an annual scenario test, testing at least one scenario A to D each year on a rotating basis.

9.7 The authorised bank must confirm to the Bank details of the results of its annual scenario test within one month of the test being carried out.

RULE 10

Cessation of Note Issue

Background

An authorised bank may choose to cease issuing banknotes. Once an authorised bank has voluntarily ceased issuing it loses its right to rely on section 213 of the Act (saving for existing issuers).

It may also lose the right to rely on section 213 by virtue of a Treasury determination to that effect (see section 223(1) and (4)), a loss of Part 4 permission under the Financial Services and Markets Act 2000 (see section 223(5)) or by virtue of insolvency (see section 220(5)). This Rule 10 relates to the circumstances other than insolvency.

The Banking Act 2009

Section 219 – Ceasing the business of issuing notes

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 11 – Cessation of note issue

Regulation 13 – Provision of information to the Bank of England

Notification

10.1 An authorised bank must, subject to any overriding legal obligation to make a disclosure, notify the Bank of an intention to cease issuing notes at least three months before any public announcement of such an intention is made.

10.2 The notification must contain:

a. the date on which it intends to make public announcement of its intention to cease issuing notes;
b. the date it intends to cease issuing notes (which must be no earlier than two months after the public announcement);
c. the reason for its decision to cease issuing notes.

Public Announcement

10.3 Before voluntarily ceasing to issue notes, an authorised bank must make a public announcement containing at least the following information:

a. the date of cessation of issue;
b. the arrangements, including timetable, for the withdrawal of the authorised bank's Notes In Circulation;
c. information on the alternative arrangements for future note provision to depositors and other customers; and
d. that backing assets will only be maintained for two years from the date of cessation of issue.

10.4 The authorised bank must make its public announcement from at least two months before the date of cessation, as a minimum, by:

a. displaying notices at each of its branches;

b. making leaflets containing the announcement available at each of its branches; and
c. publishing the announcement in media likely to be seen by its noteholders.

10.5 The authorised bank must publish the announcement at least one month prior to the date of cessation of issue:
a. in the Edinburgh Gazette, if it issues notes in Scotland; or
b. in the Belfast Gazette, if it issues note in Northern Ireland.

Loss of Issuing Rights of the Authorised Bank

10.6 The following Rules 10.7 to 10.10 apply where an authorised bank:
a. loses the right to rely on section 213 of the Act (saving for existing issuers) by virtue of:
i. a determination made by the Treasury under section 223(1)(b) (termination of right to issue);
ii. section 223(5) (loss of permission under Part 4 of the Financial Services and Markets Act 2000); or
b. becomes aware that it has reason to consider that it might lose that right by virtue of such circumstances.

10.7 The authorised bank must immediately;
a. notify the Bank that it has lost the right to rely on section 213 or (as the case may be) that it has reason to consider that it might do so; and
b. provide details of the circumstances by virtue of which it has lost or that it has reason to consider that it might lose that right.

10.8 The authorised bank must apply to the Bank if it wishes the Bank to permit the authorised bank to issue notes for a transitional period in accordance with regulation 12, confirming the date on which it wishes the transitional period to start and end.

10.9 Upon losing the right to rely on section 213 of the Act in the circumstances referred to in Rule 10.6, the authorised bank must make a public announcement containing at least the following information:
a. the fact that the authorised bank has lost the right to issue notes by virtue of such circumstances;
b. the date of the end of any transitional period;
c. the arrangements, including timetable, for the withdrawal of the authorised bank's Notes In Circulation;
d. information on the alternative arrangements for future note provision to depositors and other customers;
e. that backing assets will only be maintained for two years from the date that the authorised bank lost its right under section 213 of the Act;
f. such other information as may assist the public with obtaining value in exchange for notes of the authorised bank.

10.10 The authorised bank must make the public announcement, as a minimum, by:
a. displaying notices at each of its branches;
b. making leaflets containing the announcement available at each of its branches; and
c. publishing the announcement:
i. in media likely to be seen by its noteholders; and

ii. in the Edinburgh Gazette, if it issues notes in Scotland; or
iii. in the Belfast Gazette, if it issues notes in Northern Ireland.

Following Cessation

10.11 The authorised bank must promptly destroy or arrange for destruction of its notes which are:
a. in its possession on the date of cessation of issue; or
b. subsequently returned to its possession.

10.12 The authorised bank must make suitable arrangements with other financial institutions, representatives of the cash handling industry and major retailers for the withdrawal from circulation of the authorised bank's notes from the date of cessation of issue.

10.13 If, during the two year period following the date of cessation of issue, the authorised bank enters an insolvency process the requirements of this Rule 10 shall cease to apply.

Commentary

i Cessation of note issuing means ceasing issuing all designs and denominations that the authorised bank issues.

ii "Insolvency process" is defined in regulation 19(1).

iii The date of cessation of issue is the date on which the authorised bank ceases to put its own notes into, or back into, circulation.

RULE 11

Note Exchange Programme

Background

In the event of an authorised bank entering an insolvency process (see Part 6 of the Regulations) the Bank is responsible for managing a note exchange programme. These Rules will provide the Bank with the information it needs to run the programme and to help maintain confidence in the remaining authorised banks' notes. This includes requiring information about note specification and detection equipment for all authorised banks, so that the Bank is fully prepared to make arrangements for a note exchange programme at any time.

The Banking Act 2009

Section 220 – Insolvency, &c.

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 3 – Rules

Regulation 21 – Note exchange programme

Regulation 22 – Rights of noteholders

Regulation 23 – Backing assets

Regulation 24 – Note exchange programme: commencement and duration

Regulation 25 – Unissued banknotes

Regulation 26 – Rules relating to a note exchange programme and destruction of banknotes

Regulation 27 – Temporary continuation of note issuing after insolvency

Regulation 28 – Notes issues after loss of note issuing rights

11.1 The provisions of Rules 11.2 to 11.4 apply to an authorised bank which enters an insolvency process.

11.2 The authorised bank must cooperate with and facilitate the arrangements of the note exchange programme to be administered by the Bank.

11.3 The authorised bank must provide the Bank with immediate access to all its backing assets and unissued notes.

11.4 The authorised bank must not use, move or otherwise deal with or permit any use of, movement of or other dealing with its backing assets or unissued notes without the consent of the Bank.

Specifications

11.5 The provisions of rules 11.6 to 11.8 apply to all authorised banks.

11.6 An authorised bank must provide the Bank with the detailed specifications of all the series of its notes currently in issue and, where it intends to issue a new series, prior to issuing any such new series. Specifications are to include all security features (overt, machine-readable, and others).

11.7 An authorised bank must provide the Bank with details of the detection equipment on its sorting machines for its notes.

11.8 An authorised bank must provide the Bank with a copy of its mutilated notes policy and procedures and any update or revision to the policy.

Loss of Issuing Right of Another Authorised Bank

11.9 Where an authorised bank has lost issuing rights because it has become insolvent, other authorised banks must (upon the Bank making arrangements for reimbursement for the face value of notes collected):

a. give such assistance as the Bank may reasonably request in operating a note exchange programme;
b. if requested by the Bank, exchange the notes of the affected bank:
   i. subject to them having sufficient of their own notes available to comply, for their own notes; or
   ii. otherwise, for value in such form as the Bank reasonably requests, and
c. if requested by the Bank and in accordance with such reasonable instructions as the Bank may give, dispose of the notes it receives.

Commentary

i If an authorised bank enters into an insolvency process, the Bank will make arrangements for a note exchange programme. Any note exchange programme will need to be tailored to the particular circumstances of the authorised bank in the insolvency process. In all cases, the aims will be to help ensure that noteholder claims are satisfied and that there are sufficient notes in circulation.

ii Rule 11 includes provisions under which the Bank can make requests of other authorised banks to play a role in the note exchange programme and the disposal of notes. Also, under the Regulations, the Bank can give directions about backing assets (regulation 23) and unissued banknotes (regulation 25(1)(b)). The Bank could, for example, give directions about the destruction of notes which are not in issue.

.

RULE 12

Appeals Relating to Penalties

Background

This rule supplements the provisions in Schedule 3 to the Regulations. Where the Bank gives a decision notice to impose a penalty, the authorised bank has the opportunity for the matter to be considered by an Appeal Panel of the Bank. Where this occurs, the decision notice is suspended for the duration of the appeal.

The Banking Act 2009

Section 222 – Financial penalty

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 3 – Rules

Regulation 33 – Penalties

Schedule 3 – Imposition of penalties

12.1 This Rule 12 applies where an authorised bank has received notice under:

a. paragraph 1 of Schedule 3 of the Regulations (notice of proposal); or
b. paragraph 2 of that Schedule (variation of proposal).

12.2 Where the Bank gives notice under paragraph 3 of that Schedule (decision notice), it must also specify in the decision notice:

a. that the authorised bank may, in writing, apply to the Bank for the matter to be considered by an Appeal Panel ("an appeal");
b. the period in which the application can be made (which must be a period of not less than 14 days from the date the notice is received by the authorised bank); and
c. that if the authorised bank applies for an appeal the decision notice is suspended.

12.3 Where the authorised bank applies in writing for an appeal within the period specified in the decision notice:

a. the Bank shall arrange for the matter to be considered by an Appeal Panel; and
b. the decision notice is suspended until:
    i. the Appeal Panel makes a finding, at which point the decision notice ceases to have effect (the Bank may issue a further decision notice if the finding allows); or
    ii. the authorised bank confirms that it is no longer pursuing the appeal.

12.4 An Appeal Panel shall comprise three persons:

a. a member of Court or officer or servant of the Bank, who must be a person who has not been involved in a decision to which the decision notice relates (including any decision relating to a notice which preceded the decision notice) ("the Bank member");
b. two persons who are not members of Court or officers or servants of the Bank ("the external members").

12.5 The Bank member shall chair the Appeal Panel.

12.6 At least one of the external members shall be a person whom the Bank considers to have relevant experience of banking or the regulation of financial institutions.

12.7 Parties may attend and be represented by legal advisors at hearings before the Appeal Panel. The Appeal Panel may deliberate matters in the absence of the parties.

12.8 At any hearing before the Appeal Panel, the chair of the Panel may:

a. give such directions as he or she considers appropriate for the fair determination of the issues; and
b. as appropriate, appoint times and places for further hearings before the Appeal Panel.

12.9 The Appeal Panel may give directions without a hearing.

12.10 Directions may include (but are not limited to) the following:

a. the production of reports or other material to assist the Appeal Panel to reach a decision;
b. the making of written representations;
c. the making of oral representations at a hearing or hearings;
d. the attendance of witnesses at a hearing or hearings and their examination and/or cross-examination (on oath or otherwise).

12.11 A finding of the Appeal Panel may include that the penalty should remain the same, be reduced, be increased or that a penalty should not be imposed in respect of the subject matter of the appeal.

12.12 The Bank shall take steps in accordance with the finding of the Appeal Panel, which may include, as appropriate issuing a variation of proposal under paragraph 2 of Schedule 3 to the Regulations or a decision notice under paragraph 3 of that schedule.

12.13 The requirements of Rule 12.2 do not apply to decision notices given following the appeal process (including a decision notice which follows a variation of proposal).

Commentary

i The Appeal Panel will comprise the Bank member as both Chair and decision maker, and two external members. One of the external members will be a person whom the Bank considers to have relevant experience of banking or the regulation of financial institutions. The second external member is likely to be a person without a direct connection with the banking industry (and with no current professional connection). It may, for example, be a person with relevant legal experience. A list of Appeal Panel members appears on the Bank's website.

ii The Appeal Panel will determine what is disclosed concerning the content of its findings. However, the Bank would expect that, ordinarily, this would include detailed reasons and, where the appeal panel considers it appropriate, an outline of dissenting views.

SCHEDULE

NIPS CODE OF CONNECTION: NCS AND S&NI REMOTE ACCESS END POINT REQUIREMENTS – 2011

Introduction

Notes Circulation Scheme Members (NCS) and Scotland and Northern Ireland issuing bank users need to access the Bank of England NIPS portal from locations outside of the jurisdiction of the Bank of England.

The following Code of Connection sets out the controls that the Bank of England requires external organisations apply to their end-point devices, used to access the NIPS system, in order for them to be considered a Managed Device. Only Managed Devices may access the NIPS system.

For the purposes of this Code of Connection, a Managed Device is an Organisation's corporate Windows desktop PC, Laptop or workstation that is managed to a corporate standard aligned to IT Security industry good practice. If an Organisation proposes to use a managed device which does meet this definition they must contact the Bank of England for guidance.

The Compliance report set out at Appendix B represents a self certification from each organisation as to their compliance with the Code of Connection. This will be an annual process as required by Rules 6.8 and 6.11 (Annex 21, Appendix B) in the Rules of the Note Circulation Scheme 2011 and Rule 8.4 of the Scottish & Northern Ireland Banknote Rules 2011 and Statement of Penalty Policy.

Access types

It is highly important to the Bank to protect its networks and services from the risks that arise from allowing remote access to them. Remote access extends the organisational boundary of the Bank's network into remote locations where the end point resides.

Every remote access service allows data exchanges between the remote end point and the Bank's network and if the end point is compromised then it could introduce an unauthorised path into the Bank. Controls must therefore be placed around the end point, the network and the communications path between the two.

The following controls are designed to help the Bank assess your compliance with the Bank's end point security requirements. They align to industry good practice and the Bank considers them necessary to maintain a secure remote access service.

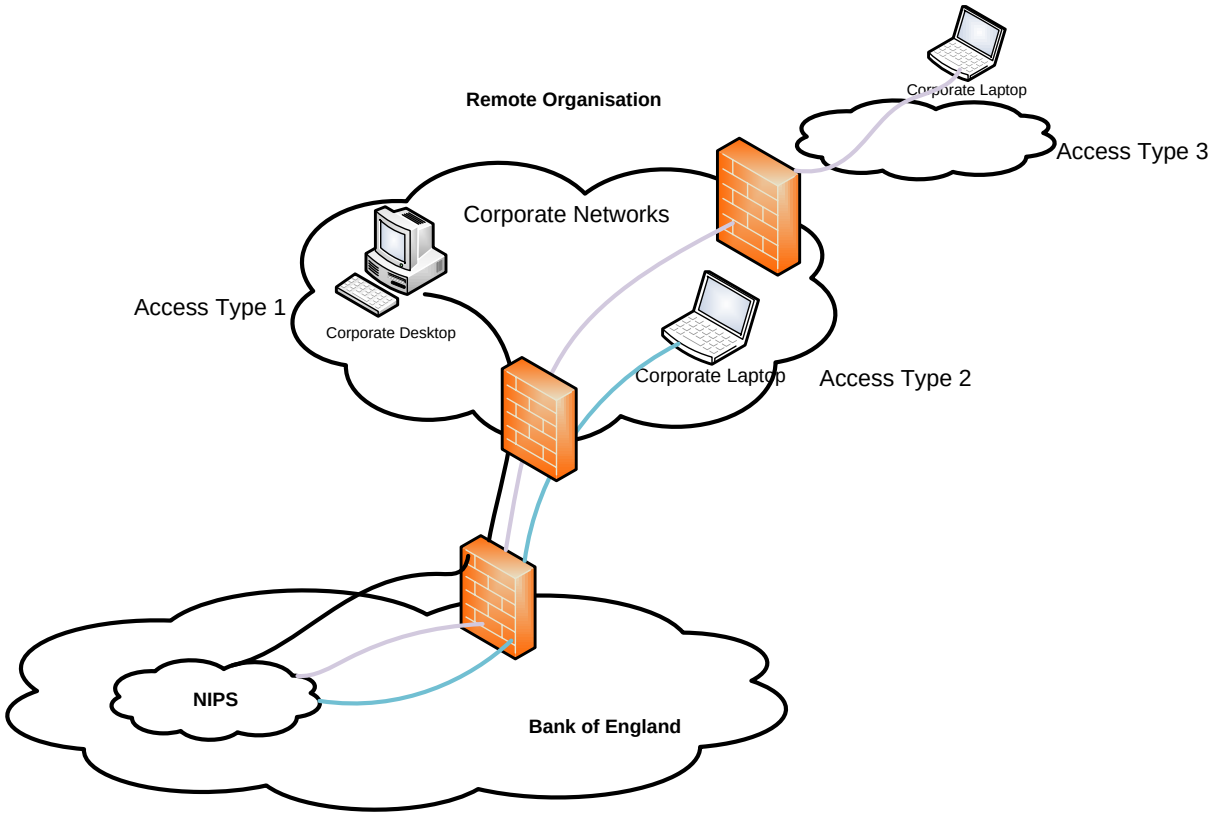
The following sections define the controls required around three types of remote access from managed devices:

1. Access based on an organisation's desktop solution, connecting to the Banks NIPS portal through the remote organisation's corporate network infrastructure;

2. Access based on an organisation's laptop solution, connected to the remote organisation's internal network and connecting to the Bank's NIPS portal through the organisation's corporate network infrastructure;

3. Access based on an organisation's laptop solution, remotely connecting to the organisation's network via a remote access solution and then connecting to the Bank's NIPS portal through the organisation's corporate network infrastructure.

The diagram below illustrates these three different types of access:



An organisation may use any or all of these access types to connect to the NIPS portal. If you have a solution which does not match those outlined here then please contact the Bank of England for guidance.

Access type 1: Connections to the Bank's NIPS portal through the use of a fully managed organisation desktop PC connecting via a DMZ infrastructure.

1. PHYSICAL END POINT DEVICE INTEGRITY:

1.1. Access must be from end points issued by the Organisation or their outsourced partner (personal machines must not be used);

1.2. Each Organisation must have a documented computer usage policy which describes the procedural and physical controls that ensure that end points are under the control of the Organisation at all times;

1.3. All end points and networking equipment must be located in a secure location;

1.4. Communications technologies such as Bluetooth, IrDA or wireless networking must be disabled at all times.

1.5. The BIOS of the end point device must be password protected to prevent unauthorised access and configured to prevent the end point from booting from any device other than the internal HDD

2. LOGICAL CONTROL:

2.1. All end points must be hardened in line with an Organisational operating system security guide, or a recognised hardening guideline such as those from the NSA[1] or Microsoft;

2.2. The end point must be locked down as far as possible so that only the required services and functionality is allowed to run;

2.3. All manufacturer software patches and updates must be applied in accordance with the Organisation's patch management and configuration control policies. These policies must define patching cycles which allow for the deployment of patches as soon as practically possible and for the deployment of critical patches outside of the normal cycle;

2.4. Applications installed on the end point should be limited to only those which are required for the defined business purposes of the Organisation;

2.5. Anti-virus / anti-malware software must be installed on the end point with the signature database updated on a regular (e.g. daily) basis;

2.6. Both the network and the desktop environments must identify and block viruses, malware and dangerous file types;

---

[1] The NSA Windows XP Security Guide can be found here (in Zip format): http://www.nsa.gov/ia/_files/os/winxp/Windows_XP_Security_Guide_v2.2.zip

2.7. Users must run with the minimum privileges required to perform the business function, ideally at the user level of a standard Windows account. Users must be prevented from modifying any security settings or installing new applications or software on the end point;

2.8. For normal users, administrative access must be enabled through the provision of a second, separate account which is specifically used to perform privileged functions, or carried out by a separate administrative business function;

2.9. Access to removable media such as USB devices, CD's or multi-media cards must be restricted and only allowed where there is a strong business requirement. Tools to control this access and enforce encryption policies or read / write access must be deployed;

3. COMMUNICATIONS SECURITY:

3.1. The Organisation must deploy a suitable DMZ infrastructure to protect its own internal network, this should include layered firewalls, content management and intrusion detection / prevention systems;

3.2. End points connecting to the Bank's NIPs portal must be NAT'd at the perimeter of the Organisation's DMZ infrastructure so as to present a designated IP address or range of addresses which can be registered with the Bank for the purposes of white-listing in our firewalls.

4. **AUTHENTICATION:**

4.1. A user must authenticate to the Organisation's network in order to access the services of the Organisation and subsequent access to the NIPS portal;

4.2. All users must be assigned a unique username and all passwords must be applied on a per user basis, not per terminal or per Organisation;

4.3. At all levels, strong passwords must be used in the authentication process. In this instance a strong password is: at least 8 characters (14 for administrators), alpha numeric with at least one numeric in all passwords. Where this requirement has not been met, mitigating controls in line with the Organisation's own policy may be accepted (please detail);

4.4. A password policy must be applied on all devices which enforces password length, minimum and maximum password ages (e.g. 1 day and 30 days respectively) and password history (e.g. 12 passwords before re-use);

4.5. Passwords used to authenticate users at any level must not be written down or shared.

5. AUDIT AND MONITORING:

5.1. The Organisation must assist the Bank by reporting lost or stolen Bank issued tokens;

5.2. Compliance reporting must be running to monitor configuration and patch deployment. Reporting must identify to the Organisation those end points which fail to comply with the Organisation’s policy;

5.3. Desktop PC configuration must be checked against the Organisation’s standards every 12 months and any deviations rectified;

Access type 2: Connections to the Bank's NIPS portal through the use of a managed corporate laptop directly attached to the organisations internal network and connecting via a DMZ infrastructure.

1. PHYSICAL END POINT DEVICE INTEGRITY:

1.1. Access must be from end points issued by the Organisation or their outsourced partner (personal machines must not be used);

1.2. Each Organisation must have a documented computer usage policy which describes the procedural and physical controls that ensure the end point is under the control of the user or organisation at all times; this includes procedures for securing the end point when not in use;

1.3. Users should be given clear instructions for looking after the end point and educated in the risks that may arise from tampering with or losing the device. This should include a process that allows users to report loss or compromise without fear of penalty;

1.4. All end points and networking equipment must be located in a secure location;

1.5. Communications technologies such as Bluetooth and IrDA should be disabled or restricted to known business connections at all times;

1.6. Wireless connectivity may only be used to connect to known internal access points or those which conform to the configurations detailed in appendix A;

1.7. The BIOS of the end point device must be password protected to prevent unauthorised access and configured to prevent the end point from booting from any device other than the internal HDD.

2. LOGICAL CONTROL:

2.1. All end points must be hardened in line with an Organisational operating system security guide, or a recognised hardening guideline such as those published by the NSA[2] or Microsoft;

2.2. The end point should be locked down as far as possible so that only the required services and functionality is allowed to run;

2.3. All manufacturer software patches and updates must be applied in accordance with the Organisation's patch management and configuration control policies. These policies must define patching cycles which allow for

[2] The NSA Windows XP Security Guide can be found here (in Zip format): http://www.nsa.gov/ia/_files/os/winxp/Windows_XP_Security_Guide_v2.2.zip

the deployment of patches as soon as practically possible and for the deployment of critical patches outside of the normal cycle;

2.4. Applications installed on the end point should be limited to only those which are required for the defined business purposes of the Organisation;

2.5. Anti-virus /anti-malware software must be installed on the end point with the signature database updated on a regular (e.g. daily) basis;

2.6. Both the network and the laptop environments must identify and block viruses, malware and dangerous file types;

2.7. Users must run with the minimum privileges required to perform the business function, ideally at the user level of a standard Windows account. Users must be prevented from modifying any security settings or installing new applications or software on the end point;

2.8. For normal users, administrative access must be enabled through the provision of a second, separate account which is specifically used to perform privileged functions, or carried out by a separate administrative business function;

2.9. Whole disk encryption must be used on the end point hard drive to protect data at rest. Where possible this should be CAPS approved, accredited to FIPS 140-2 L2 or recognised as suitable for the protection of HMG Restricted data;

2.10. Access to removable media such as USB devices, CD's or multi-media cards must be restricted and only allowed where there is a strong business requirement. Tools to control this access and enforce encryption policies or read / write access should be deployed.

3. COMMUNICATIONS SECURITY:

3.1. The end point must have a software firewall installed which includes policies that restrict access to the Internet or any other trusted third party network other than for the purposes of connecting into a corporate remote access solution. (i.e. the end point must first connect to the corporate network and all subsequent activity must be routed via this connection);

3.2. The Organisation must deploy a suitable DMZ infrastructure to protect its own internal network, this should include layered firewalls, content management and intrusion detection systems;

3.3. End points connecting to the Bank's NIPs portal must be NAT'd at the perimeter of the Organisation's DMZ infrastructure so as to present a designated IP address or range of addresses which can be registered with the Bank for the purposes of white-listing in our firewalls.

4. **AUTHENTICATION:**

4.1. As hard disk encryption products are mandated, users must authenticate to these products before the end point will boot into the installed operating system;

4.2. A user must authenticate to the Organisation's network in order to access the services provided on that network and subsequent access to the NIPS portal;

4.3. All users must be assigned a unique username and all passwords must be applied on a per user basis, not per terminal or per Organisation;

4.4. At all levels, strong passwords must be used in the authentication process. In this instance a strong password is: at least 8 characters (14 for administrators), alpha numeric with at least one numeric in all passwords. Where this requirement has not been met, mitigating controls in line with the Organisation's own policy may be accepted (please detail);

4.5. A password policy must be applied on all devices which enforces password length, minimum and maximum password ages (e.g. 1 day and 30 days respectively) and password history (e.g. 12 passwords before re-use);

4.6. Passwords used to authenticate users at any level must not be written down or shared.

5. AUDIT AND MONITORING:

5.1. The Organisation must assist the Bank by reporting lost or stolen Bank issued tokens;

5.2. Compliance reporting must be running to monitor configuration and patch deployment. Reporting must identify to the Organisation those end points which fail to comply with the Organisation's policy;

5.3. End point configuration must be checked against the Organisation's standards every 12 months and any deviations rectified;

Access type 3: Connections to the Bank's NIPS portal through the use of a managed corporate laptop remotely connected to the organisation but using the organisations DMZ infrastructure for onward access:

1. PHYSICAL DEVICE INTEGRITY:

1.1. Access must be from end points issued by the Organisation or their outsourced partner (personal machines must not be used);

1.2. Each Organisation must have documented remote working and computer usage policies. These must describe locations where it is or is not acceptable to use the end point and the procedural and physical controls that ensure that end points are under the control of the user or Organisation at all times. The policies must also include procedures for securing the end point when not in use;

1.3. Users should be given clear instructions for looking after the end point and educated in the risks that may arise from tampering with or losing the device. This should include a process that allows users to report loss or compromise without fear of penalty;

1.4. All networking equipment must be located in a secure location;

1.5. Communications technologies such as Bluetooth and IrDA should be disabled or restricted to known business connections at all times;

1.6. Wireless connectivity may only be used to connect to known / trusted access points or those which conform to the configurations detailed in appendix A;

1.7. The BIOS of the end point device must be password protected to prevent unauthorised access and configured to prevent the laptop from booting from any device other than the internal HDD.

2. LOGICAL CONTROL:

2.1. All end points must be hardened in line with an Organisational operating system security guide, or a recognised hardening guideline such as those published by the NSA[3] or Microsoft;

2.2. The endpoint should be locked down as far as possible so that only the required services are allowed to run;

2.3. All manufacturer software patches and updates must be applied in accordance with the Organisation's patch management and configuration control policies. These policies must define patching cycles which allow for

[3] The NSA Windows XP Security Guide can be found here (in Zip format): http://www.nsa.gov/ia/_files/os/winxp/Windows_XP_Security_Guide_v2.2.zip

the deployment of patches as soon as practically possible and for the deployment of critical patches outside of the normal cycle;

2.4. Applications installed on the end point should be limited to only those which are required for the defined business purposes of the Organisation or remote access to the Organisation's network;

2.5. Anti-virus / anti-malware software must be installed on the end point with the signature database updated on a regular (e.g. daily) basis;

2.6. Both the network and the end point environments must identify and block viruses, malware and dangerous file types;

2.7. Users must run with the minimum privileges required to perform the business function, ideally at the user level of a standard Windows account. Users must be prevented from modifying any security settings or installing new applications or software on the laptop;

2.8. For normal users, administrative access must be enabled through the provision of a second, separate account which is specifically used to perform privileged functions, or carried out by a separate administrative business function;

2.9. Whole disk encryption must be used on the end point hard drive to protect data at rest, where possible this should be CAPS approved, accredited to FIPS 140-2 L2 or recognised as suitable for the protection of HMG Restricted data;

2.10. Access to removable media such as USB devices, CD's or multi-media cards must be restricted and only allowed where there is a strong business requirement. Tools to control this access and enforce encryption policies or read write access should be deployed.

3. COMMUNICATIONS SECURITY:

3.1. The end point must have a software firewall installed which includes policies that restrict access to the Internet or any other trusted third party network other than for the purposes of connecting into a corporate remote access solution. (i.e. the client device must first securely connect to the corporate network and all subsequent activity must be routed via this connection);

3.2. Appropriate IPSec or SSL end to end encryption must be used between the laptop and the boundary access point of the Organisation's network;

3.3. The Organisation must deploy a suitable DMZ infrastructure to protect its own internal network, this should include layered firewalls, content management and intrusion detection systems;

3.4. End Points connecting to the Bank's NIPs portal must be NAT'd at the perimeter of the Organisation's DMZ infrastructure so as to present a designated IP address or range of addresses which can be registered with the Bank for the purposes of white-listing in our firewalls.

4. AUTHENTICATION:

4.1. As hard disk encryption products are mandated, users must authenticate to these products before the end point will boot into the installed operating system;

4.2. A user must authenticate to the organisation's network in order to access the services of the member Organisation and subsequent access to the NIPS portal;

4.3. When establishing the VPN used to connect the laptop to the member Organisation's remote working solution, the end point and the network must authenticate each other (typically by means of a VPN application which supports mutual authentication);

4.4. All users must be assigned a unique username and all passwords must be applied on a per user basis, not per terminal or per Organisation;

4.5. Two factor authentication between the client and the Organisation must be used;

4.6. At all levels, strong passwords must be used in the authentication process. In this instance a strong password is: at least 8 characters (14 for administrators), alpha numeric with at least one numeric in all passwords. Where this requirement has not been met, mitigating controls in line with the Organisation's own policy may be accepted (Please detail);

4.7. A password policy must be applied on all devices which enforces password length, minimum and maximum password ages (e.g. 1 day and 30 days respectively) and password history (e.g. 12 passwords before re-use);

4.8. Passwords used to authenticate users at any level must not be written down or shared.

5. AUDIT AND MONITORING:

5.1. The Organisation must assist the Bank by reporting lost or stolen Bank issued tokens;

5.2. Compliance reporting must be running to monitor configuration and patch deployment. Reporting must identify to the Organisation those end points which fail to comply with the Organisation’s policy;

5.3. End point configuration must be checked against the Organisation’s standards every 12 months and any deviations rectified;

5.4. The auditing and monitoring policy of the member Organisation must record all remote connection activity, including both successful and unsuccessful connection requests. All activity must be attributable to an individual.

APPENDIX A – WIRELESS ACCESS POINT CONFIGURATION:

1. Wireless devices used must be Wi-Fi certified, and must implement WPA2 security.

2. 802.1X authentication must be used.

3. EAP-TLS must be used for authentication, using X.509v3 certificates for both user and endpoint authentication. Other protocols must be disabled at the access point and at the client.

4. Mutual authentication must be used. Clients must be configured not to connect to ad hoc networks.

5. AES-CCMP must be used for confidentiality and integrity.

6. WEP and TKIP must be disabled at the access point, and the client if possible, to prevent WPA2 connections from falling back to these encryption modes.

7. WPA2 authentication is not sufficient to grant access privileges to network services. Network services must be protected by auxiliary security measures (see 4.5).

8. System security policies should set a maximum duration for the validity of the pairwise master key which must not exceed 1 day or 248 – 1 bytes, whichever is first. Devices which do not enforce an appropriate re-keying period must not be used.

9. Procedures must be set down and enforced to ensure that the WPA2 connection has been initiated correctly before it is used to pass RESTRICTED material.

10. Endpoint certificates must not be used for user authentication.

11. Certificates granting access to a network carrying RESTRICTED traffic are considered RESTRICTED ACCSEC and must be protected in accordance with CESG policy for protection of such material.

12. The network SSID must be broadcast, and must not be set to the manufacturer's default value.

13. MAC address filtering is permitted but not required.

14. Client software must be configured such that if its default protectively marked network (the "home" network) is not available then it will not attempt to locate or

connect to other networks. Client software must not respond to invitations to connect which come from networks other than the home network.

15. Users without administrative privileges must not be able to reconfigure clients to connect to other networks.

16. Technical restrictions must be in place to prevent users changing network configuration, adding, modifying or removing certificates, sharing their wireless connection via Ethernet and creating, modifying or removing firewall rules.

17. Wireless access to the access point's administration interface (via HTTP, SSH, Telnet etc.) must be disabled.

18. All default usernames and passwords for all network equipment must be changed.

19. Firewalls and ACLs must be put in place to restrict access to access points, the RADIUS server, wireless clients and additional network servers, including file and print servers.

20. When patches become available for access points, RADIUS servers, wireless client software, wireless card drivers and firmware and operating systems, those patches must be applied.

21. A certificate revocation process must be implemented. In the event that a wireless client is lost, stolen or compromised, its endpoint and user certificates must be revoked.

APPENDIX B – COMPLIANCE REPORT: AND SELF CERTIFICATION

SECTION 1 – DECLARATION:

We confirm that the answers below are a true and accurate reflection of our organisations compliance with the NIPS Code of Connection 2011[4].

ORGANISATION: AND SCHEME (NCS/S&NI)	
ACCREDITOR NAME: **ACCREDITOR SIGNATURE:** **DATE:**	
BUSINESS AUTHORISER NAME: **BUSINESS AUTHORISER SIGNATURE:** **DATE:**	

[4] As required by Rules 6.8 and 6.11 (Annex 21, Appendix B) in the Rules of the Note Circulation Scheme 2011 and Rule 8.4 of the Scottish & Northern Ireland Banknote Rules 2011 and Statement of Penalty Policy.

SECTION 2 – YOUR ACCESS ROUTES :

Please describe how your organisation connects to the Bank's NIPS portal:
Please describe your organisations internal security policy and governance arrangements (e.g. ISO 27002 based)

SECTION 3 – COMPLIANCE WITH ACCESS TYPE 1 CONTROLS: : Connections to the Bank's NIPS portal through the use of a fully managed organisation desktop PC connecting via a DMZ infrastructure

IF YOUR ORGANISATION DOES NOT USE THIS MODE OF CONNECTION PLEASE ENTER NOT APPLICABLE

Section	No.	Control	Compliant?	Comments
1	1	**PHYSICAL DEVICE INTEGRITY**		
	1.1	Access must be from end points issued by the Organisation or their outsourced partner (Personal machines must not be used);	Yes / No / Partial	
	1.2	Each Organisation must have a documented computer usage policy which describes the procedural and physical controls that ensure that end points are under the control of the Organisation at all times;		
	1.3	All end points and networking equipment must be located in a secure location;		
	1.4	Communications technologies such as Bluetooth, IrDA or wireless networking must be disabled at all times.		
	1.5	The BIOS of the end point device must be password protected to prevent unauthorised access and configured to prevent the end point from booting from any device other than the internal HDD		
1	2	**LOGICAL CONTROL**		
	2.1	All end points must be hardened in line with an Organisational operating system security guide, or a recognised hardening guideline such as those from the NSA or Microsoft;		
	2.2	The end point must be locked down as far as possible so that only the required services and functionality is allowed to run;		
	2.3	All manufacturer software patches and updates must be applied in accordance with the Organisation's patch management and configuration control policies. These policies must define patching cycles which allow for the deployment of patches as soon as practically possible and for the deployment of critical patches outside of the normal cycle;		
	2.4	Applications installed on the end point should be limited to only those which are required for the defined business purposes of the Organisation;		
	2.5	Anti-virus / anti-malware software must be installed on the		

		end point with the signature database updated on a regular (e.g. daily) basis;		
	2.6	Both the network and the desktop environments must identify and block viruses, malware and dangerous file types;		
	2.7	Users must run with the minimum privileges required to perform the business function, ideally at the user level of a standard Windows account. Users must be prevented from modifying any security settings or installing new applications or software on the end point;		
	2.8	For normal users, administrative access must be enabled through the provision of a second, separate account which is specifically used to perform privileged functions, or carried out by a separate administrative business function;		
	2.9	Access to removable media such as USB devices, CD's or multi-media cards must be restricted and only allowed where there is a strong business requirement. Tools to control this access and enforce encryption policies or read / write access must be deployed;		
1	**3**	**COMMUNICATIONS SECURITY**		
	3.1	The Organisation must deploy a suitable DMZ infrastructure to protect its own internal network, this should include layered firewalls, content management and intrusion detection / prevention systems;		
	3.2	End Points connecting to the Bank's NIPs portal must be NAT'd at the perimeter of the Organisation's DMZ infrastructure so as to present a designated IP address or range of addresses which can be registered with the Bank for the purposes of white-listing in our firewalls.		
1	**4**	**AUTHENTICATION**		
	4.1	A user must authenticate to the Organisation's network in order to access the services of the Organisation and subsequent access to the NIPS portal;		
	4.2	All users must be assigned a unique username and all passwords must be applied on a per user basis, not per terminal or per Organisation;		
	4.3	At all levels, strong passwords must be used in the authentication process. In this instance a strong password is: at least 8 characters (14 for administrators), alpha numeric with at least one numeric in all passwords. Where this requirement has not been met, mitigating controls in line with the Organisation's own policy may be accepted (Please detail);		

	4.4	A password policy must be applied on all devices which enforces password length, minimum and maximum password ages (e.g. 1 day and 30 days respectively) and password history (e.g. 12 passwords before re-use);		
	4.5	Passwords used to authenticate users at any level must not be written down or shared.		
1	**5**	**AUDIT AND MONITORING**		
	5.1	The Organisation must assist the Bank by reporting lost or stolen Bank issued tokens;		
	5.2	Compliance reporting must be running to monitor configuration and patch deployment. Reporting must identify to the Organisation those end points which fail to comply with the Organisation's policy;		
	5.3	End point configuration must be checked against the Organisation's standards every 12 months and any deviations rectified;		

SECTION 4 – COMPLIANCE WITH ACCESS TYPE 2 CONTROLS: **Connections to the Bank's NIPS portal through the use of a managed corporate laptop directly attached to the organisations internal network and connecting via a DMZ infrastructure.**

IF YOUR ORGANISATION DOES NOT USE THIS MODE OF CONNECTION PLEASE ENTER NOT APPLICABLE

Section	No.	Control	Compliant	Comments
2	**1**	**PHYSICAL DEVICE INTEGRITY**		
	1.1	Access must be from end points issued by the Organisation or their outsourced partner (Personal machines must not be used);	Yes / No / Partial	
	1.2	Each Organisation must have a documented computer usage policy which describes the procedural and physical controls that ensure the end point is under the control of the user or organisation at all times; this includes procedures for securing the end point when not in use;		
	1.3	Users should be given clear instructions for looking after the end point and educated in the risks that may arise from tampering with or losing the device. This should include a process that allows users to report loss or compromise without fear of penalty;		
	1.4	All end points and networking equipment must be located in a secure location;		
	1.5	Communications technologies such as Bluetooth and IrDA should be disabled or restricted to known business connections at all times;		
	1.6	Wireless connectivity may only be used to connect to known internal access points or those which conform to the configurations detailed in appendix A;		
	1.7	The BIOS of the end point device must be password protected to prevent unauthorised access and configured to prevent the end point from booting from any device other than the internal HDD.		
2	**2**	**LOGICAL CONTROL**		
	2.1	All end points must be hardened in line with an Organisational operating system security guide, or a recognised hardening guideline such as those published by the NSA or Microsoft;		
	2.2	The end point should be locked down as far as possible so that only the required services and functionality is allowed to run;		

	2.3	All manufacturer software patches and updates must be applied in accordance with the Organisation's patch management and configuration control policies. These policies must define patching cycles which allow for the deployment of patches as soon as practically possible and for the deployment of critical patches outside of the normal cycle;		
	2.4	Applications installed on the end point should be limited to only those which are required for the defined business purposes of the Organisation;		
	2.5	Anti-virus / anti-malware software must be installed on the end point with the signature database updated on a regular (e.g. daily) basis;		
	2.6	Both the network and the laptop environments must identify and block viruses, malware and dangerous file types;		
	2.7	Users must run with the minimum privileges required to perform the business function, ideally at the user level of a standard Windows account. Users must be prevented from modifying any security settings or installing new applications or software on the end point;		
	2.8	For normal users, administrative access must be enabled through the provision of a second, separate account which is specifically used to perform privileged functions, or carried out by a separate administrative business function;		
	2.9	Whole disk encryption must be used on the end point hard drive to protect data at rest. Where possible this should be CAPS approved, accredited to FIPS 140-2 L2 or recognised as suitable for the protection of HMG Restricted data;		
	2.10	Access to removable media such as USB devices, CD's or multi-media cards must be restricted and only allowed where there is a strong business requirement. Tools to control this access and enforce encryption policies or read / write access should be deployed.		
2	**3**	**COMMUNICATIONS SECURITY**		
	3.1	The end point must have a software firewall installed which includes policies that restrict access to the Internet or any other trusted third party network other than for the purposes of connecting into a corporate remote access solution. (I.e. the end point must first connect to the corporate network and all subsequent activity must be routed via this connection);		
	3.2	The Organisation must deploy a suitable DMZ infrastructure to protect its own internal network, this		

		should include layered firewalls, content management and intrusion detection systems;		
	3.3	End Points connecting to the Bank's NIPs portal must be NAT'd at the perimeter of the Organisation's DMZ infrastructure so as to present a designated IP address or range of addresses which can be registered with the Bank for the purposes of white-listing in our firewalls.		
2	**4**	**AUTHENTICATION**		
	4.1	As hard disk encryption products are mandated, users must authenticate to these products before the end point will boot into the installed operating system;		
	4.2	A user must authenticate to the Organisation's network in order to access the services provided on that network and subsequent access to the NIPS portal;		
	4.3	All users must be assigned a unique username and all passwords must be applied on a per user basis, not per terminal or per Organisation;		
	4.4	At all levels, strong passwords must be used in the authentication process. In this instance a strong password is: at least 8 characters (14 for administrators), alpha numeric with at least one numeric in all passwords. Where this requirement has not been met, mitigating controls in line with the Organisation's own policy may be accepted (Please detail);		
	4.5	A password policy must be applied on all devices which enforces password length, minimum and maximum password ages (e.g. 1 day and 30 days respectively) and password history (e.g. 12 passwords before re-use);		
	4.6	Passwords used to authenticate users at any level must not be written down or shared.		
2	**5**	**AUDIT AND MONITORING**		
	5.1	The Organisation must assist the Bank by reporting lost or stolen Bank issued tokens;		
	5.2	Compliance reporting must be running to monitor configuration and patch deployment. Reporting must identify to the Organisation those end points which fail to comply with the Organisation's policy;		
	5.3	End point configuration must be checked against the Organisation's standards every 12 months and any deviations rectified;		

SECTION 5 – COMPLIANCE WITH ACCESS TYPE 3 CONTROLS: **Connections to the Bank's NIPS portal through the use of a managed corporate laptop remotely connected to the organisation but using the organisations DMZ infrastructure for onward access.**

IF YOUR ORGANISATION DOES NOT USE THIS MODE OF CONNECTION PLEASE ENTER : NOT APPLICABLE

Section	No.	Control	Compliant	Comments
3	**1**	**PHYSICAL DEVICE INTEGRITY**		
	1.1	Access must be from end points issued by the Organisation or their outsourced partner (Personal machines must not be used);	Yes / No / Partial	
	1.2	Each Organisation must have documented remote working and computer usage policies. These must describe locations where it is or is not acceptable to use the end point and the procedural and physical controls that ensure that end points are under the control of the user or Organisation at all times. The policies must also include procedures for securing the end point when not in use;		
	1.3	Users should be given clear instructions for looking after the end point and educated in the risks that may arise from tampering with or losing the device. This should include a process that allows users to report loss or compromise without fear of penalty;		
	1.4	All networking equipment must be located in a secure location;		
	1.5	Communications technologies such as Bluetooth and IrDA should be disabled or restricted to known business connections at all times;		
	1.6	Wireless connectivity may only be used to connect to known / trusted access points or those which conform to the configurations detailed in appendix A;		
	1.7	The BIOS of the end point device must be password protected to prevent unauthorised access and configured to prevent the laptop from booting from any device other than the internal HDD.		
3	**2**	**LOGICAL CONTROL**		

	2.1	All end points must be hardened in line with an Organisational operating system security guide, or a recognised hardening guideline such as those published by the NSA or Microsoft;		
	2.2	The endpoint should be locked down as far as possible so that only the required services are allowed to run;		
	2.3	All manufacturer software patches and updates must be applied in accordance with the Organisation's patch management and configuration control policies. These policies must define patching cycles which allow for the deployment of patches as soon as practically possible and for the deployment of critical patches outside of the normal cycle;		
	2.4	Applications installed on the end point should be limited to only those which are required for the defined business purposes of the Organisation or remote access to the Organisation's network;		
	2.5	Anti-virus / anti-malware software must be installed on the end point with the signature database updated on a regular (e.g. daily) basis;		
	2.6	Both the network and the end point environments must identify and block viruses, malware and dangerous file types;		
	2.7	Users must run with the minimum privileges required to perform the business function, ideally at the user level of a standard Windows account. Users must be prevented from modifying any security settings or installing new applications or software on the laptop;		
	2.8	For normal users, administrative access must be enabled through the provision of a second, separate account which is specifically used to perform privileged functions, or carried out by a separate administrative business function;		
	2.9	Whole disk encryption must be used on the end point hard drive to protect data at rest, where possible this should be CAPS approved, accredited to FIPS 140-2 L2 or recognised as suitable for the protection of HMG Restricted data;		
	2.10	Access to removable media such as USB devices, CD's or multi-media cards must be restricted and only allowed		

		where there is a strong business requirement. Tools to control this access and enforce encryption policies or read–write access should be deployed.		
3	**3**	**COMMUNICATIONS SECURITY**		
	3.1	The end point must have a software firewall installed which includes policies that restrict access to the Internet or any other trusted third party network other than for the purposes of connecting into a corporate remote access solution. (I.e. the client device must first securely connect to the corporate network and all subsequent activity must be routed via this connection);		
	3.2	Appropriate IPSec or SSL end to end encryption must be used between the laptop and the boundary access point of the Organisation's network;		
	3.3	The Organisation must deploy a suitable DMZ infrastructure to protect its own internal network, this should include layered firewalls, content management and intrusion detection systems;		
	3.4	End Points connecting to the Bank's NIPs portal must be NAT'd at the perimeter of the Organisation's DMZ infrastructure so as to present a designated IP address or range of addresses which can be registered with the Bank for the purposes of white-listing in our firewalls.		
3	**4**	**AUTHENTICATION**		
	4.1	As hard disk encryption products are mandated, users must authenticate to these products before the end point will boot into the installed operating system;		
	4.2	A user must authenticate to the organisations network in order to access the services of the member Organisation and subsequent access to the NIPS portal;		
	4.3	When establishing the VPN used to connect the laptop to the member Organisation's remote working solution, the end point and the network must authenticate each other (typically by means of a VPN application which supports mutual authentication);		
	4.4	All users must be assigned a unique username and all passwords must be applied on a per user basis, not per terminal or per Organisation;		

	4.5	Two factor authentication between the client and the Organisation's network must be used before onward connection to the Bank's NIPS Portal		
	4.6	At all levels, strong passwords must be used in the authentication process. In this instance a strong password is: at least 8 characters (14 for administrators), alpha numeric with at least one numeric in all passwords. Where this requirement has not been met, mitigating controls in line with the Organisation's own policy may be accepted (Please detail);		
	4.7	A password policy must be applied on all devices which enforces password length, minimum and maximum password ages (e.g. 1 day and 30 days respectively) and password history (e.g. 12 passwords before re-use);		
	4.8	Passwords used to authenticate users at any level must not be written down or shared.		
3	**5**	**AUDIT AND MONITORING**		
	5.1	The Organisation must assist the Bank by reporting lost or stolen Bank issued tokens;		
	5.2	Compliance reporting must be running to monitor configuration and patch deployment. Reporting must identify to the Organisation those end points which fail to comply with the Organisation's policy;		
	5.3	End point configuration must be checked against the organisations standards every 12 months and any deviations rectified;		
	5.4	The auditing and monitoring policy of the member Organisation must record all remote connection activity, including both successful and unsuccessful connection requests. All activity must be attributable to an individual.		

STATEMENT OF PENALTY POLICY

Background

This is the statement of penalty policy that is required by Schedule 3, paragraph 5 of the Regulations in respect of the penalty process and the amount of any penalty that may be imposed by the Bank.

The Banking Act 2009

Section 222 – Financial Penalty

The Scottish and Northern Ireland Banknote Regulations 2009

Regulation 33 – Penalties

Schedule 3 – Imposition of penalties

1 This is a statement of the policy of the Bank of England ("the Bank") in relation to financial penalties imposed under section 222 of the Banking Act 2009 and the Scottish and Northern Ireland Banknote Regulations 2009 (the "Regulations").

2 In this statement, a failure by an authorised bank to comply with any of the Regulations or the Scottish and Northern Ireland Banknote Rules 2009, 2010 or 2011 ("the Rules") is referred to as a 'compliance failure'.

3 The Bank updates its statement of penalty policy from time to time. This statement applies in respect of a compliance failure which occurs or continues on or after 11 May 2012. The statement published on the date in the first column of table 1 applies in respect of any compliance failure which occurred or continued on or after that date but wholly before the relevant date in the second column.

Table 1

Statement of penalty policy (SPP)	Applies to compliance failures occurring or continuing on or after the date of the SPP and wholly before:
23 November 2009	1 April 2010
1 April 2010	21 May 2010
21 May 2010	24 June 2011
24 June 2011	11 May 2012

4 In deciding whether to impose a penalty, the Bank will follow the provisions of Schedule 3 to the Regulations (imposition of penalties) and Rule 12 (appeals relating to penalties).

5 The Bank may impose a financial penalty in the event of a compliance failure, subject to the limit set by the Regulations, which is based on the value of 10% of the bank's Notes In Circulation in the previous calendar year.

6 Subject to that limit, the Bank has discretion on whether to impose a penalty for a compliance failure and, if so, the amount of that penalty, and it will

exercise its discretion taking account, as appropriate, of the principles set out in this policy and all relevant circumstances of which it is aware.

7 Where repeated compliance failures have a single underlying cause, the Bank may treat those breaches as a single breach for the purposes of deciding whether a penalty is to be imposed and, if so, the amount.

8 A compliance failure resulting from any act or omission by an agent of an authorised bank will be treated as a failure by that bank.

9 The Bank's policy is, for the purpose of financial penalties, to treat compliance failures as falling into three categories ("category 1", "category 2" and "category 3").

10 A category 1 compliance failure is any compliance failure that results in either of the following situations arising:

a. the total value of the authorised bank's backing assets falling below the total value of notes required to be backed at the relevant time; or
b. the total value of the authorised bank's backing assets in the form of Bank of England notes and UK coin falling below 60% of the value of its Notes In Circulation at the relevant time.

11 A category 1 compliance failure could relate to circumstances such as under-declaration of total Notes In Circulation or Notes With the Potential to Enter Circulation; or from over-declaration of Excluded Notes or backing assets; or from a combination of these factors; or from any other form of reporting or other failure resulting in underbacking.

12 A category 2 compliance failure is a compliance failure which does not fall within any other category.

13 A category 3 compliance failure is a compliance failure constituting a breach of Rule 8.4 (the NIPS Code of Connection) which does not also constitute a breach of any other Regulation or Rule.

Penalties

General

14 Penalty amounts will be a multiple of £100.

15 The Bank will not impose a penalty where a compliance failure arises solely as a result of a technical failure of the Bank's systems.

16 The authorised bank will be expected to co-operate with the Bank in the provision of sufficient relevant, high quality information, in a timely manner to enable the Bank to undertake a proper assessment of the compliance failure.

Category 1

17 The maximum penalty in respect of a category 1 compliance failure is the highest of:

a. the difference between the total value of the authorised bank's backing assets and the total value of its notes required to be backed at the relevant time;

b. the difference between the total value of the authorised bank's backing assets in the form of Bank of England notes and UK coin and 60% of the value of its Notes In Circulation at the relevant time.

18 Where a compliance failure has occurred or persisted on more than one calendar day, the Bank may calculate the maximum penalty on the basis of the value on any one calendar day during which the compliance failure persisted.

19 The minimum penalty for a category 1 compliance failure is £20,000.

Category 2

20 The maximum penalty for a category 2 compliance failure is £20,000.

21 The Bank will take certain factors into account when determining the penalty to be imposed. In particular the Bank will take into account the following factors:

a. Whether the Bank considers that the compliance failure was proactively disclosed by the authorised bank and/or was discovered by the authorised bank or by a third party;
b. Whether the Bank considers that the compliance failure was deliberate; and
c. Whether the Bank considers that reasonable care was exercised by the authorised bank.

22 The penalty to be imposed after the consideration of these factors will be as follows:

Table 2

Nature of failure	**Reporting**	
	Compliance failure proactively disclosed by authorised bank once it is aware of the compliance failure	**Compliance failure not proactively disclosed by authorised bank once it is aware of the compliance failure**
Deliberate	**£20,000**	**£20,000**
Not deliberate but reasonable care not taken	***£10,000 (if discovered by issuing bank)*** ***£15,000 (if discovered by third party)***	***£20,000***
Not deliberate and reasonable care taken	***£5,000 (if discovered by issuing bank)*** ***£7,500 (if discovered by third party)***	***£20,000***

23 A deliberate failure includes wilful acts or omissions of individual employees or management and may include acts, omissions, approaches or practices which could reasonably be known to be in contravention of the Rules or

Regulations.

24 Where the issuing bank does not proactively disclose the compliance failure to the Bank as soon as it is aware of it, the compliance failure will attract the maximum penalty.

25 Factors which the Bank may take into account in reaching its view on whether or not reasonable care has been taken may include, but are not limited to:

- *Whether the degree of care the authorised bank employed when putting in place systems, processes and controls to comply with the new regulatory requirements. For example, whether a compliance department or another appropriate department was involved in reviewing or testing the systems, processes and controls put in place at the start of the new regime and/or on an ongoing basis.*

- *Whether the compliance failure was due to a legitimate misunderstanding / misinterpretation of the regulatory regime. The steps that the authorised bank had taken in order to develop a proper understanding of the regulatory regime may be a factor in evaluating whether a misunderstanding or misinterpretation was legitimate.*

- *Whether the authorised bank's internal processes were followed. If so, it will be necessary to consider what aspect of the authorised bank's processes allowed the compliance failure to occur.*

- *Whether the authorised bank's internal processes have been followed with due skill, care and diligence.*

- *Whether the compliance failure was clearly a one off or ad hoc error, which was exceptional to a generally careful approach taken, or, conversely, whether it was one of a series of failures.*

- *Whether other professionals in the industry also have taken the same steps.*

- *Whether the breach was caused by an arithmetical mistake. If so it will be necessary to consider the circumstances in which the mistake took place. Relevant factors may include whether there were procedures or controls in place to detect the error at a later stage and the reasons why they were not effective. The size, nature and frequency of the error may also need to be considered.*

26 The Bank will consider the total Category 2 penalty to be imposed following the application of the factors outlined in paragraphs 22 to 25, together with any additional information provided by the authorised bank. In exceptional circumstances the Bank may make further reductions to the penalty amounts outlined in Table 2 above, but would not ordinarily expect to reduce the penalty to below a sum representing:

a. any reduction in the Bank's seigniorage which may have resulted from the compliance failure; and
b. any financial or other benefit enjoyed by the authorised bank by virtue of the compliance failure.

27 Factors that the Bank is minded to take into account in the exercise of the Bank's discretion will be included in the notice of proposed penalty it gives in each case under schedule 3, paragraph 1 of the Regulations.

Category 3

28 A category 3 compliance failure does not attract a financial penalty.