RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

MUNICIPAL YEAR 2015/16

COMMITTEE:	**Item No. 5**
AUDIT COMMITTEE **7th December 2015**	**BACS Approved Bureau Scheme Report**

REPORT OF:-

GROUP DIRECTOR, CORPORATE & FRONTLINE SERVICES

Author: Marc Crumbie (Operational Audit Manager)

(01443) 680779

1. PURPOSE OF THE REPORT

In accordance with the terms of reference for Audit Committee, this report provides Members with a summary of the findings and recommendations of the finalised external triennial inspection: BACS Approved Bureau Scheme Report.

2. RECOMMENDATIONS

It is recommended that Members:

2.1 Note the conclusions, findings and recommendations contained within the Bacs Approved Bureau Scheme Report (Appendix B); and

2.2 Seek clarity and explanation if there are areas of concern.

3. BACKGROUND

3.1 All organisations that process payroll and pension payments on behalf of other Employers via Bankers' Automated Clearing Services (BACS) are subject to a triennial inspection process from the Bacs Approved Bureau Scheme. An on-site inspection of this Council took place on the 21st October 2015.

3.2 As part of the inspection process, the Council was required to complete a questionnaire and submit relevant evidence in support of its responses. The questionnaire was submitted in advance of the on-site inspection with the aim of enabling the Bureau to understand the Council and the nature of its operations. The questionnaire covers the security controls and procedures to inform an external assessment of the integrity, confidentiality and ongoing availability of Bacs services. A blank copy of the questionnaire is provided at Appendix A.

3.3 During the on-site visit, the Inspector undertook a detailed review of the information contained within the questionnaire together with a walk-around inspection of the business critical areas where BACS payments are administered. Verbal feedback was provided at the end of the inspection and this was followed-up by the Inspector's Report.

3.4 The Inspector's report contains details of the Council's security arrangements including the makes and models of IT security controls, and business critical information. For this reason, key conclusions, findings and recommendations have been included within the up date to Audit Committee rather than the full report.

4. BACS Approved Bureau Scheme Report – Conclusions

4.1 The Bacs Approved Bureau Scheme uses the following categories to grade organisations, as noted in Table 1 below.

Table 1 – Bacs Approved Bureau Scheme Categories

Category	BACS Approved Bureau
Excellent	No re-inspection required within the 3 year period.
Good	
Adequate	
Requires Improvement	Not satisfactory, a re-inspection would be arranged.

4.2 Set out at Table 2 below are the conclusions reported and Appendix B provides associated findings, recommendations and implementation timescales agreed by Management.

Table 2 - Conclusions reported

Area	**Conclusion**
Bureau organisation and financial information history	We assessed the bureau as being **GOOD** in this category
Physical security	We assessed the bureau as being **EXCELLENT** in this category.
Computer operations	We assessed the bureau as being **GOOD** in this category.
Applications and systems support	We assessed the bureau as being **EXCELLENT** in this category.
Bacs processing and operations	We assessed the bureau as being **GOOD** in this category.

4.3 Members will note that Management have agreed to implement the recommendations outlined in Appendix B and the Internal Audit Service will monitor implementation as part of existing reporting arrangements to Audit Committee.

5. SUMMARY

5.1 The Bacs Approved Bureau Inspector has completed a review of the Council's BACS operations and has categorised all of the areas examined as either Excellent or Good. It is considered that this provides assurance over the integrity and security of the Council's BACS transactions.

5.2 In doing so, it also helps Members to form an opinion on the overall control environment prior to the closure of accounts process for 2015/16.

****

LOCAL GOVERNMENT ACT, 1972

as amended by

THE ACCESS TO INFORMATION ACT, 1985

RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

LIST OF BACKGROUND PAPERS

AUDIT COMMITTEE

7th December 2015

Report of the Group Director, Corporate & Frontline Services
Author: Marc Crumbie (Operational Audit Manager).

Item		**File Ref:**
5.	BACS Approved Bureau Scheme – Final Report	IA / MC

Contact Officer: Marc Crumbie
Operational Audit Manager
Bronwydd House
Porth
CF39 9DL
Tel. No. (01443) 680779

bacs

Bacs Approved Bureau Scheme Inspection Questionnaire

Bureau details

Bureau Name:		
Bureau Number:		
Visit date(s):		
Inspector(s):		
Bureau website:		
Bureau email address:		
Do you wish to be included in BAB (Bacs Approved Bureaux) directory?	Yes ☐ No ☐	
Bureau representatives:	**Name**	**Job title**

Please complete and return this questionnaire electronically.

All shaded fields can be used for your answers. The fields will expand automatically to accommodate your response. Check boxes can be clicked on to provide answers to some questions. To deselect a check box, simply click on it again.

Version: 6.43 V5
Date: January 2011

Contents

1 Introduction

We ask you to complete this questionnaire to enable us to understand your organisation and the nature of your operations. The questionnaire covers the security controls and risk management procedures that ensure the integrity, confidentiality and ongoing availability of your Bacs services. Relevant sections are based on the Information Security Standard ISO/IEC 27001:2005.

All bureaux applying for Bacs Approved Bureau status and existing Bacs Approved Bureaux must complete this questionnaire as part of the inspection process.

The questionnaire is divided into sections relating to different aspects and the sections can be distributed to the relevant managers. In order to ensure a fair and comprehensive evaluation, it is important that you answer all questions (unless there are specific instructions otherwise). Please note some questions require descriptive answers and space has been given for your responses. Should you require extra space, please attach your replies on a separate and clearly referenced sheet of paper.

All information will be treated confidentially and will not be disclosed without your prior written consent to any third party other than Bacs Payment Schemes Limited and your sponsoring bank. We will keep all documents and other confidential information at our usual place of business in the United Kingdom.

During the inspection visit, we will confirm and clarify your responses by observation and discussion. We will analyse the responses, using our predefined scoring system, taking into account the size and nature of your bureau.

Please email the completed questionnaire and supporting documentation to the bureau inspector at least two weeks before the inspection visit. A checklist is provided on page 6.

Please retain a copy of the completed questionnaire for your reference.

Further information, including Bacs Inspection Guidelines, is available on the Bacs website at www.bacs.co.uk

If you have any queries, please contact the commercial bureaux inspection team at Commercial Bureaux Support, Bacs Payment Schemes Limited, 2 Thomas More Square, London, E1W 1YN or via the "Contact us" page on the Bacs website (www.bacs.co.uk select "Bureaux" and then "Contact us") or click the following hyperlink Contact us

Disclaimer

Please note that the assessment covers the technical competence and operational integrity of the bureau in accordance with the requirements of the Scheme. Bacs Payment Schemes Limited (Bacs) does not undertake any assessment nor make any representation in respect of the suitability or otherwise of any approved bureaux for any purpose.

Glossary

For the purpose of this questionnaire, the following terms will be used as defined below.

Term	Definition
Account limit	The maximum value that can be paid from (credits) or collected into (debits) an individual account or group of accounts during a period set by your sponsor without creating an overlimit referral. Your sponsor sets the account limit.
ADDACS	Automated Direct Debit And Cancellation Service Refer Bacs Reports
Additional Contact	A type of contact able to act for a service user on Bacstel-IP. Additional contacts cannot be given any privileges to maintain their service user or other contacts.
Alternative Security Method (ASM)	An access method using a user-id and password to provide secure access to the Bacs payment services website that can only be used for the collection of Bacs reports. (To do certain things on the website, you need to use Public Key Infrastructure security.)
ARUCS	Automated Return of Unapplied Credits Service Refer Bacs Reports
ARUDD	Automated Return of Unpaid Direct Debits Refer Bacs Reports
AUDDIS	Automated Direct Debit Instruction Service Refer Bacs Reports
AWACS	Advice of Wrong account for Automated Credits Service Refer Bacs Reports
Bacs	The electronic funds transfer system operated by VocaLink Limited on behalf of Bacs Payment Schemes Limited.
Bacs Approved Software Service	An approval service to make sure that all software used with Bacstel-IP meets set requirements. You can only use software to access Bacstel-IP that is approved under this service.
Bacs Reports	These reports are normally collected by your clients/customers from the Bacs Payment Services web site.
Bacstel-IP	A service providing a secure access for the Bacs service. It uses internet technologies and PKI security. You access Bacstel-IP either using payment services or Bacs approved software for Bacstel-IP.
Bacstel-IP software	In this guide, Bacstel-IP software refers to software that has been approved under the Bacs Approved Software Service for Bacstel-IP.
BASS	See Bacs Approved Software Service
Bureau	A bureau submits payment files to the Bacs service for other service users. Bureaux that submit for third parties must be certified as a Bacs Approved Bureau. A bureau is a type of direct submitter.

Contact	A person that can act for a service user. There are two types of contacts: Primary Security Contacts (PSCs) and Additional Contacts (ACs).
DDICA	Direct Debit Indemnity Claims Advice Refer Bacs Reports
Digital certificate	Assigned by a trusted certificate authority, a digital certificate is the form in which PKI credentials are issued. In Bacstel-IP terms, certificates are normally held on a smartcard, but can also be held on an HSM (Hardware Security Module).
Digitally sign	You digitally sign information using a smartcard or an HSM. This produces a digital signature that is attached to the file or message before it is sent. This digital signature allows the receiver to identify the sender and tell if the contents of the file or message have been altered after it was signed.
Hardware Security Module	A piece of hardware installed into your computer systems that holds PKI credentials. HSMs allow you to automate the submission and report collection process.
HSM	See Hardware Security Module
Input report	A report that the Bacs service produces following the processing of payment information for a particular service user for a particular day. Any payments that have been amended, rejected or returned are highlighted on the report. Using Bacstel-IP, you can access input reports within 4 hours of processing.
Payment file	A set of payment instructions that are submitted to the Bacs service for processing. A payment file is sent as part of a submission. You can optionally digitally sign payment files.
PKI	See Public Key Infrastructure
Primary Security Contact	A type of contact linked to a service user. Direct submitters must have at least two PSCs; indirect submitters do not have to have any PSCs. A PSC can be given a wider range of privileges than an additional contact, including the privilege to be able to add and maintain Additional Contacts.
PSC	See Primary Security Contact
Public Key Infrastructure	A system to verify the validity of parties involved in electronic communications and to secure electronic data transmissions. PKI uses two “keys”: a public and a private key. A message encrypted with a private key can only be decrypted with the associated public key (and vice versa).
PKI credentials	The collective term for the public and private keys issued to an individual in the form of a digital certificate. PKI credentials are used for authentication and encryption. A trusted certificate authority issues them.
Smartcard	A card with an embedded microchip that is used to store a contact’s PKI credentials. The smartcard is used to authenticate the holder and digitally sign data.
Sponsor	The bank or building society that has authorised your service user to use the Bacs service.

Submission	A payment file or files transmitted to the Bacs service for processing. All submissions sent to Bacstel-IP must be digitally signed using PKI credentials.
Transaction application(s)	Software applications that are used to process transactions and to generate data that will be imported into the Bacstel-IP application, for example, payroll or financial accounting packages.

Checklist

To allow as full an assessment as possible, please have available for viewing the following documentation where appropriate and available. The references below relate to questions in this questionnaire.

Please click on the boxes to check/uncheck it as appropriate to indicate if the documentation is available at the review (R) or if a copy is attached (A) to the questionnaire.

R	A	Sec.	Documentation
□	□	2.4	Organisation chart
□	□	2.7	Employment contract
□	□	2.7	Information and IT Security policies
□	□	2.8	Personnel policies and procedures
□	□	2.9	Internal audit reports relating to Bacs systems and processing
□	□	2.9	External audit reports relating to Bacs systems and processing
□	□	2.10	Quality accreditation registrations
□	□	3.2	Accounts
□	□	4.2	Client contracts including areas with specific Bacs service responsibilities
□	□	4.3	Professional indemnity insurance policy certificate
□	□	7	Computer configuration/network diagram
□	□	8	Logical access control procedures (if not contained in Information and IT Security policies)
□	□	10.11	Business continuity/disaster recovery plan/procedures
□	□	11	Application change control procedures
□	□	12-16	Documented procedures for the scheduling, production, control and monitoring of Bacs related files and Bacs submissions.

2 Organisation and policy

This section covers organisation, policies and issues of security and control. We wish to identify organisations whose areas of responsibility are well defined and adequately resourced with proper attention paid to personnel, security and control issues.

2.1 Describe the structure and principle activities of your organisation.

2.2 What is the legal status of your organisation? (For example Plc, Limited company, Partnership, LLP, Local authority)

2.3 Describe the ownership structure of your organisation, for example 100% owned by its two directors/partners/other individuals; wholly owned subsidiary of XYZ Plc.

2.4 Please attach a chart of the organisation structure of your organisation, down to the level of manager responsible for the Bacs bureau operations, indicating the number of personnel in each area.

Chart attached? Yes □ No □

2.5 Please complete the matrix below giving the job titles of the managers responsible for the areas listed.

Definitions:

- **Customer Liaison** - agreeing commercial and operation arrangements and resolving operational problems with clients/customers.
- **Bacs and Bank Liaison** - agreeing operational arrangements and resolving operational problems.
- **Computer Operations -** managing the operation of the computer installation and/or network.
- **Data Control** - ensuring that data is correctly handled and distributed before and after processing.
- **Systems Development** - managing the creation and maintenance of applications software developed in-house and/or managing the installation of third-party software products.
- **Security Administration (Logical) -** managing access control to data assets and all aspects of their protection.
- **Security Administration (Physical)** - managing access control to physical assets and all aspects of their protection.
- **Contingency Planning** - ensuring that operations can be reinstated in case of a serious incident or disaster.

Name/Job title/Location	Customer Liaison	Bacs & Bank Liaison	Data Control	Computer Operations	Systems Development	Logical Security Admin	Physical Security Admin	Contingency Planning
	□	□	□	□	□	□	□	□
	□	□	□	□	□	□	□	□
	□	□	□	□	□	□	□	□
	□	□	□	□	□	□	□	□
	□	□	□	□	□	□	□	□
	□	□	□	□	□	□	□	□

2.6 What provision is made in the departments listed in question 2.5 for holidays and unexpected personnel absence?

2.7 Do you have a contract of employment for personnel?

Contract? Yes □ No □ Copy attached? Yes □ No □

How is it kept up to date to reflect statutory requirements?

Do you have procedures covering the following areas? Please attach copies.

Grievance procedures	Yes □	No □
Disciplinary procedures	Yes □	No □
Termination and dismissal procedures	Yes □	No □
Confidentiality policy	Yes □	No □

Do you have Information and IT Security policies, which cover Internet and e-mail usage, computer use and misuse including password usage and control?

Yes □ No □

Are these policies included within your contract of employment?

Yes □ No □

Where are the policies and procedures maintained? (For example staff handbook, Intranet)

2.8 Do your contracts and personnel/HR policies cover the following areas? Please attach copies if available.

Job descriptions	Yes □	No □	Copy attached?	Yes □	No □
Recruitment checks for new employees	Yes □	No □	Copy attached?	Yes □	No □
Training and induction	Yes □	No □	Copy attached?	Yes □	No □
Security awareness and education	Yes □	No □	Copy attached?	Yes □	No □

2.9 What audits and reviews are undertaken of your Bacs-related operations? Please attach copies.

Internal audit	Yes □	No □	Copy attached?	Yes □	No □
External audit	Yes □	No □	Copy attached?	Yes □	No □
SAS 70	Yes □	No □	Copy attached?	Yes □	No □
Other	Yes □	No □	Copy attached?	Yes □	No □

If other, please specify:

2.10 Does your organisation have any formal quality accreditations? Please supply copies of any accreditation certificates.

ISO 9001:200x or equivalent	Yes □	No □
ISO/IEC 27001:200x	Yes □	No □
Investor in People	Yes □	No □
TickIT	Yes □	No □
ICAEW or ICAS guidelines	Yes □	No □
Internal Quality Management Standards	Yes □	No □
Quality Management Systems	Yes □	No □
Other	Yes □	No □

If other, please specify:

2.11 Are you required to maintain a current notification under the Data Protection Act?

Notification required	Yes □	No □
If yes, have you registered your notification?	Yes □	No □

3 Financial information

The purpose of this section is to obtain financial information regarding your business and holding companies (where appropriate).

3.1 How long has your organisation been in operation?

Number of years:		Or since (year):	

3.2 Please attach a copy of the latest audited accounts.

If your company is a subsidiary, please also attach the audited accounts of the holding company.

Accounts attached? Yes □ No □

Details:

3.3 What is your annual turnover?

Annual turnover (£):	

3.4 What approximate percentage of your annual turnover do your two largest clients/customers contribute?

Percentage (%):	

3.5 What approximate percentage of your annual income comes from clients/customers using your Bacs services?

Percentage (%):	

4 Commercial arrangements

This section examines your relationship with your clients/customers to establish that responsibilities and liabilities are clearly defined.

4.1 How many clients/customers use your bureau services to have payments made through Bacs?

No. of client/ customers:	

How many clients/customers that use your bureau services do not have payments made through Bacs?

No. of client/ customers:	

4.2 Do you have written contracts or letters of engagement with your clients/customers?

Yes □ No □

If yes, do the contracts or letters of engagement describe Bacs-specific responsibilities, for example a service level agreement? Please attach a sample.

Describe Bacs-specific responsibilities? Yes □ No □ Sample attached? Yes □ No □

4.3 Do you have business or professional indemnity insurance? Please attach a copy of the certificate.

Insurance? Yes □ No □ Copy attached? Yes □ No □

Details:

4.4 Do you have insurance cover for the following?

Direct loss: damage to equipment or buildings? Yes □ No □

Indirect loss of business, increased cost of working? Yes □ No □

5 Professional services

This section gathers information about the services that you provide. Its purpose is to enable us assess the risk associated with your Bacs business.

5.1 What percentages of your Bacs processing do the following represent? Please specify transaction types, for example purchase ledger credits.

Transaction types	Percentage by volume
Direct Credit	
Direct Debit	

5.2 How long have you been providing Bacs bureau services?

Number of years: Or since (year):

5.3 How many transactions have you submitted to Bacs in the last three years? If necessary, the Bacs Inspector can supply this information at the review. Applicant bureaux should provide an estimate of the expected level of annual transactions.

Number of transactions last year:	
Number of transactions two years ago:	
Number of transactions three years ago:	

5.4 Do you provide accounting with bank reconciliation services for any Bacs users?

Yes □ No □

If yes, please describe these services and details of any independent reviews of the accounts.

5.5 Are Bacs payments funded or paid:

From/to bank accounts controlled by your clients/customers?	Yes □	No □
From/to bank accounts controlled by your organisation?	Yes □	No □

6 Physical security

This section covers the physical security of your bureau operations. We are seeking to establish that access to them is well controlled and that they are properly protected from hazards such as fire, flood or malicious damage.

Part I: Premises description and physical access controls

6.1 Please provide a general description of the premises in which the Bacs bureau operations are conducted and controlled

6.2 Is your building shared with other organisations?

Yes □ No □

Please list any other organisations that share your building and indicate the nature of their business.

Company name	Type of business

If your building is shared, how is access to your working areas protected?

6.3 How is employee access to the building containing your Bacs bureau facilities controlled?

How is access to the building controlled outside normal working hours?

6.4 How is visitor access controlled?

Do visitors sign-in and out? Are visitor badges issued?

6.5 Do you have a separate Bacs Operations area within your organisation?

Yes □ No □

If yes, please provide details

Do you further restrict access to the Bacs Operations area?

Yes □ No □

If yes, how and to whom?

6.6 Do you have a separate Bacs Transmission area within your organisation?

Yes □ No □

If yes, please provide details

Do you further restrict access to the Bacs Transmission area?

Yes □ No □

If yes, how and to whom?

6.7 Are your main network servers or mainframe computers located within a designated computer room?

Yes □ No □

Please provide details describing their location

Do you further restrict access to the computer room?

Yes □ No □

If yes, how and to whom?

What procedures are there for administering the above access controls and are they documented?

How often are computer room access rights reviewed?

What is the procedure for granting access to visitors to the computer room and do you retain a separate documented record of visitors to the computer room?

Part II: Intruder detection

6.8 Is an intruder alarm fitted? If so, is it connected to the police or a monitoring service?

Alarm fitted? Yes □ No □ Monitored? Yes □ No □

6.9 What CCTV coverage do you have? Does it cover the main entrances and key internal areas, such as the computer room?

Is it recorded? If so, how long are the recordings retained?

Recorded? Yes □ No □ Time retained:

6.10 Please describe any additional security measures in place, for example security patrols?

Part III: Fire control

6.11 What smoke or fire detection and control measures are installed in the building containing the Bacs bureau facilities?

Are they monitored?

Yes □ No □

6.12 Please supply details of any smoke or fire detection equipment in the computer/server room.

6.13 Please describe any fire control system installed in the computer room, for example inert gas flooding.

6.14 What environmental monitoring devices are installed in the computer room, for example water detection or temperature control monitors?

6.15 Have the environmental risks of the computer and bureau sites been evaluated, for example buildings within a flood zone?

Yes □ No □

If yes, by whom and what recommendations were made and implemented as a result?

Part IV: General

6.16 What procedures do you have for identifying and dealing with suspect postal items received at your premises and are they documented? What training is given to personnel?

6.17 What procedures do you have for disposal of confidential paper waste and redundant computer related material and are they documented?

6.18 If collected by a third-party, is a certificate of secure destruction obtained?

Yes □ No □

7 Computer facilities and networks

In this section we ask for information about your computer facilities to enable us to interpret your responses to later sections. We will also take account of the risk arising from networks or distributed processing.

7.1 Please describe your organisation's internal computing environment, for example PC workstations operating under a combination of Windows XP (SP2) and Windows 7 that connect over an Ethernet local area network to file servers operating under a mixture of Windows server 2003/2008 with Windows Exchange 2008 e-mail Server.

7.2 Do you use a wireless network?

Yes □ No □

If yes, what security protocol do you use?

WEP □ WPA □ WPA2 □

If you use a wireless network does it provide access to your local area network (LAN)?

Yes □ No □

7.3 Please describe all external connections to/from your organisation's internal computing environment, for example a 2 Mbps broadband connection provides access to the internet, and the local area network connects to a wide area network, based on private wires (2 Mbps – 10 Mbps); support personnel can connect remotely using VPN connections and security tokens.

7.4 How does your organisation connect to the Bacs service, for example the Internet?

7.5 Please provide details of any hardware and/or software firewalls protecting your organisation's internal computing environment.

7.6 Please provide details of any anti-virus, spyware or mail scanning software used.

7.7 What transaction application(s) generates the data files that your organisation transmits to Bacs?

What Bacs transmission software does your organisation use?

7.8 Please describe where transaction data, Bacs transmission software and the transaction application(s) reside, for example PC, server, mainframe.

8 Logical access control

This section is designed to ensure that use of the Bacs applications is restricted to authorised users only. We are looking for organisations that enforce good security disciplines and procedures, with emphasis on passwords, network control and compliance checks.

8.1 What security software does your organisation use to control logical access to your PCs, servers, mainframe, the transaction and Bacs transmission application(s)?

8.2 How often, and by whom, are user accounts and access rights reviewed for the network, systems and applications?

8.3 Who authorises the setup of, and changes to, access rights for the network, systems and applications?

8.4 How is the authorisation in 8.3 communicated and recorded?

8.5 Who implements the setup of new users and changes to access rights? How is this authority restricted?

8.6 What procedures do you have for ensuring all access rights are curtailed for personnel leaving your company and are they documented?

8.7 How is the user authorisation verified, for example authorisation activity log reviewed by the security manager?

8.8 Is access of users suspended during extended periods of absence?

Yes □ No □

8.9 Please describe the logical access control methods that you use, for example passwords, biometrics and/or smartcards.

8.10 Please complete the following table to detail how network and application passwords are managed.

	Network/application			
Password requirements	**PC/network**	**Mainframe**	**Transaction application**	**Bacstel-IP software**
Change frequency				
Password reuse prevented	Yes □ No□	Yes □ No□	Yes □ No□	Yes □ No□
Number of passwords that cannot be reused				
Minimum length (characters)				
Alpha & non-alpha characters required	Yes □ No□	Yes □ No□	Yes □ No□	Yes □ No□
Special characters? (e.g.! @ # *)	Yes □ No□	Yes □ No□	Yes □ No□	Yes □ No□
Password differs from user ID	Yes □ No□	Yes □ No□	Yes □ No□	Yes □ No□
Mix of upper/lower case alpha	Yes □ No□	Yes □ No□	Yes □ No□	Yes □ No□

8.11 Does your organisation automate the control of password changes and format?

Yes □ No □

If no, how do you enforce them?

8.12 Are any passwords shared by any of the following? That is, are any passwords known to or legitimately used by two or more:

Employees?	Yes □	No □
Clients/customers?	Yes □	No □
System administrators?	Yes □	No □
Technical support personnel?	Yes □	No □
Maintenance engineers?	Yes □	No □
Others?	Yes □	No □

If others, please specify:

8.13 Are all passwords under the sole control of their owner, or does another person, such as a system administrator, have knowledge of or access to passwords? "Sole control" of a password means that only the owner knows the password and no other system user can determine it.

Yes □ No □

If no, who also has knowledge or access?

8.14 What procedures do you have for controlling the resetting of forgotten passwords and are they documented?

8.15 Do any personnel, including technical personnel, have access to editing software that facilitates the direct manipulation of data?

Yes □ No □

If yes, please provide details.

8.16 Does your organisation use password protected screensavers or other similar timeout facilities?

Yes □ No □

If yes, please provide details including timeout period.

8.17 How is access to your computers by external support engineers controlled? What passwords and telecommunications facilities do they use, and how is their use controlled?

8.18 Are user accounts or user IDs disabled after successive access control failures, for example incorrect password? Please provide details of failed attempts allowed.

Accounts disabled? Yes □ No □ Number of failures permitted:

What procedure and what level of authorisation are required to re-enable them and is the procedure documented?

8.19 Have you commissioned any external network penetration tests of your system? If yes, please provide copies of the reports.

Yes □ No □ Reports attached? Yes □ No □

9 Computer operations

In this section we examine your computer operations to verify that operators have adequate instructions and support, and that storage media are handled properly, so that unexpected problems can be managed with the minimum impact.

9.1 Has your organisation experienced any major disruption to its computer operations in the last 12 months?

Yes □ No □

If yes, please provide details including any periods of downtime.

9.2 Is your computer hardware covered by a maintenance contract and, if so, what is the guaranteed response time and hours of cover?

Hardware contract? Yes □ No □

Response time: Hours of cover:

9.3 Is any air-conditioning protecting your computer hardware covered by a maintenance contract and, if so, what is the guaranteed response time and hours of cover?

Contract? Yes □ No □

Response time: Hours of cover:

9.4 Please provide details of your hardware review and renewal policy.

9.5 Please complete the following table, detailing the audit logs that your organisation maintains and reviews.

System/function	Maintained	Reviewed	Reviewed by	Frequency
Firewall security	Yes □ No□	Yes □ No□		
Network security	Yes □ No□	Yes □ No□		
Operator activity	Yes □ No□	Yes □ No□		
Transaction application journal	Yes □ No□	Yes □ No□		
Bacstel-IP software journal	Yes □ No□	Yes □ No□		
Other	Yes □ No□	Yes □ No□		

9.6 Describe your procedures for the recording and resolution of IT security incidents. Are the procedures documented?

10 Business continuity

This section examines how you would cope if an incident ranging from a minor failure to a major systems problem or a disaster, such as fire or flood, were to affect your operations. We wish to identify that organisations can show they have considered all aspects of, and demonstrated their ability to cope with, such a situation.

10.1 What is your policy for creating data backups, including Bacs related data? Please include details of frequency and retention periods.

10.2 What is your policy for creating system and application backups and at what frequency are backups created? Please include details of frequency and retention periods.

10.3 Please describe backup media and storage, for example disks, tapes, online storage, mirroring.

Offsite:

Onsite:

10.4 How are backups secured on and off site?

10.5 What procedures do you have for controlling the issue and use of backup media and are they documented?

10.6 What is your procedure for testing backups to ensure that you can restore the system or data files and is it documented?

Are the tests recorded?

Yes □ No □

bacs

10.7 Is an uninterruptible power supply (UPS) connected to your hardware, for example mainframe, servers, Bacs transmission computer? Is a standby generator available? For how long would power be available?

UPS? Yes □ No □ Standby generator? Yes □ No □

How long?

10.8 What onsite resilience do you have for your computer equipment?

10.9 What alternative offsite provisions have you made for the following:

- Computer hardware
- Office accommodation
- Access to Bacstel-IP
- Smartcard
- Smartcard reader
- Alternate HSM solution (if appropriate)?

10.10 Do you have a disaster recovery and/or business continuity plan that details the procedures for recovery from a partial or total loss of IT and business services in a controlled manner? Please provide a copy of the plan.

Have a plan? Yes □ No □ Plan attached? Yes □ No □

10.11 Is the plan:

Documented? Yes □ No □

Circulated to key personnel? Yes □ No □

Available off site? Yes □ No □

10.12 Who has responsibility for deciding to invoke the plan(s)?

10.13 How long would it take to resume service?

10.14 What is your policy for testing your disaster recovery and/or business continuity plan and does it include a test or live Bacs transmission? Please provide the date of the last successful disaster recovery and/or business continuity test.

10.15 **What is your policy for reappraising the disaster recovery and/or business continuity plan to ensure that it is kept up to date?**

11 Application and systems support

In this section we seek to establish that there are appropriate controls over the computer and network operating systems and other systems software to minimise the risk of disruption.

11.1 Please describe your change control procedures for managing the timely implementation of critical, non-critical and major updates to operating and application software. Are the procedures documented?

Critical updates, for example security patches or updates to virus definitions:

Non-critical updates, for example service packs and optional features:

Major updates, for example version changes and implementation of new application or operating system software:

11.2 What level of approval is required before major updates are permitted? Is the approval written and retained?

Approval level:

Written & retained? Yes □ No □

11.3 What procedures do you have in place to ensure that only authorised software is in use and is covered by sufficient licences, for example software audits? Are the procedures documented?

Third party application software

11.4 Do you have maintenance contracts for third party application software?

Yes □ No □

11.5 Describe your procedures for testing new third party application software and amendments to existing application software. Are the procedures documented?

11.6 Do you modify any third party Bacs related application software, other than making changes to standard user definable parameters?

Yes □ No □

<u>If you do not have an in-house Bacs related application development function, please move to Section 12</u>

In-house application development

11.7 What systems development methodology do you use and how is it documented?

11.8 Are your change control procedures documented and do they cover?

Testing?	Yes □	No □
User acceptance and sign-off?	Yes □	No □
Documentation?	Yes □	No □

11.9 Is development work performed in a separate environment from production work?

Yes □ No □

11.10 Is the movement of files between the development and production areas and access to the live environment strictly controlled?

Yes □ No □

12 Customer data controls

This section addresses the process for handling Bacs-related client/customer data and the controls that ensure that it is properly processed and checked to protect against potential fraud.

12.1 Please estimate the source of the data generated by the transaction application for submission to the Bacs clearing.

Source	% By volume
Input by bureau personnel from information supplied by clients/customers	
Input by clients/customers	
Standing data, ie regenerated automatically on a regular frequency	
Transmitted and imported directly	
Other (please specify below)	

12.2 Please estimate how your bureau receives the data that bureau personnel input.

Source	% By volume
Email	
Fax	
Hand delivery	
Post	
Telephone	
Secure transfer, ie by FTP, web portal etc (please specify below)	
Other (please specify below)	

12.3 Do you have a clear processing schedule with your clients/customers for the delivery of data?

Yes □ No □

12.4 Are clients/customers responsible for delivering transaction data to the bureau?

Yes □ No □

12.5 What procedures ensure that data has been sent by an authorised client/customer contact and are they documented?

12.6 What procedures do you have in place to record the receipt of client/customer data? Are the procedures documented?

12.7 What procedures do you have in place to ensure that input data is validated for completeness, accuracy and integrity, for example independently verified. Are the procedures documented?

12.8 What controls ensure that client/customer data is not lost, omitted from processing or processed twice, for example a control sheet? Are the controls documented?

13 Production of Bacs data

This section covers the controls over the production of Bacs data.

13.1 Does the transaction application that initially receives or originates Bacs transaction data, produce:

Total numbers for debit and credit transactions?	Yes □	No □
Total values of debit and credit transactions?	Yes □	No □
Exceptional transactions list?	Yes □	No □
Full transaction list?	Yes □	No □
Other control totals (please specify below)?	Yes □	No □

13.2 Does the Bacstel-IP software produce?

Total numbers for debit and credit transactions?	Yes □	No □
Total values of debit and credit transactions?	Yes □	No □
Control totals for individual clients/customers?	Yes □	No □
Details of rejected transactions?	Yes □	No □
Other control totals (please specify below)?	Yes □	No □

13.3 How are the control totals reconciled?

Manually? Yes □ No □ Automatically? Yes □ No □

Who is responsible for the reconciliation?

Job title?	

Is the reconciliation recorded?

Yes □ No □

13.4 Is your organisation responsible for monitoring predefined client/customer account limits?

Yes □ No □

13.5 Is responsibility for monitoring predefined client/customer account limits contractually allocated?

Yes □ No □

14 Bacstel-IP transmission controls

In this section we examine how your organisation uses the controls Bacstel-IP provides to ensure the secure transfer of data to the Bacs clearing.

14.1 Please list your primary security contacts and additional contacts in the table below:

Please inform us separately if there are additional PSCs and ACs.			**Privileges**			
Name	**Job title**	**Smartcard**	**Signing**	**Submitting**	**Accessing reports**	**Maintain & view service users and contacts**

Primary Security Contacts:

		□	□	□	□	□
		□	□	□	□	□
		□	□	□	□	□
		□	□	□	□	□

Additional Contacts:

		□	□	□	□	N/A
		□	□	□	□	N/A
		□	□	□	□	N/A
		□	□	□	□	N/A
		□	□	□	□	N/A
		□	□	□	□	N/A

14.2 Who maintains your Bacstel-IP service user and contact details, for example telephone numbers, postal and email addresses?

14.3 What procedures do you have for the set up, maintenance and removal of PSCs and ACs and are they documented?

14.4 How do you ensure the secure retention of smartcards?

14.5 How do you ensure that PIN code knowledge and smartcards are not shared?

14.6 Do you use the Alternate Security Method (ASM) facility to collect Bacs reports from the Bacs Payment Services web site? If you do, what procedures cover the change of any ASM passwords and are they documented?

14.7 What procedures do you have to ensure timely transfer of data to Bacs and are they documented?

14.8 Please provide details of any separation of input and transmission functions.

14.9 Who explicitly authorises Bacs submissions?

15 Hardware security module (HSM) option

The HSM option provides automatic digital signing facilities for Bacstel-IP transmissions. If you do not use this option, skip this section.

Risks considered are that unauthorised transactions may be processed; systems may be abused or used fraudulently; systems may fail.

<u>If you do not use HSM please move to Section 16</u>

15.1 What HSM product model do you use?

15.2 Who holds the designated organisational roles?

Role	**Name**	**Job title**
Key Manager		
Physical Security Manager		
Application Administrator		
Auditor		

15.3 Are the PKI credentials and cryptographic keys (user credentials) held on?

HSM? Yes □ No □

Encrypted hard disk? Yes □ No □

Other (please specify below)? Yes □ No □

15.4 The Bacstel-IP subscriber standard requires a key management log. Please provide this log for review at the inspection.

Log attached? Yes □ No □

15.5 Where is any backup HSM located and how is it secured?

15.6 Where is the backup cryptographic key held and how is it secured?

15.7 What are your procedures for the disposal and decommissioning of any redundant HSM hardware?

15.8 What are your procedures for the disposal of any redundant cryptographic keys?

16 Verification of Bacs processing

Various Bacs reconciliation reports are produced to verify that client/customer data has been processed accurately. This section looks at how the reports are used and at the procedures for reconciling the reports and resolving any problems in a timely manner.

16.1 What procedures do you have for checking the Bacs Submissions Summary report and are they documented?

16.2 Is responsibility for the receipt and verification of the following report types contractually allocated?

Input report	Yes □	No □	
ARUCS (Automated Return of Unapplied Credits Service) report	Yes □	No □	N/a □
AWACS (Advice of Wrong account for Automated Credits Service) report	Yes □	No □	N/a □
ARUDD (Automated Return of Unpaid Direct Debits) report	Yes □	No □	N/a □
AUDDIS (Automated Direct Debit Instruction Service) report	Yes □	No □	N/a □
ADDACS (Automated Direct Debit And Cancellation Service) report	Yes □	No □	N/a □
DDICA (Direct Debit Indemnity Claim Advice) report	Yes □	No □	N/a □

16.3 What are your procedures for dealing with reports that you access on behalf of any of your clients/customers and are they documented?

16.4 What procedures do you have for dealing with rejected or returned items and are they documented?

16.5 What procedures do you have for extracting payment files transmitted in error and verifying withdrawal reports and are they documented?

End of questionnaire.

APPENDIX B - CONCLUSIONS, FINDINGS AND ASSOCIATED RECOMMENDATIONS

Area	Conclusion	Findings	Recommendation	Implementation date
Bureau organisation and financial information history	We assessed the bureau as being **GOOD** in this category	We understand that all clients (Service Users) are issued with and required to sign a contract which, for Bacs Service Users, is complemented by a Service Level Agreement, detailing the Council's and clients' responsibilities relating to the payroll/pensions and Bacs service. The agreement covers the majority of recommended activities, including, data delivery, data verification, checking Bacs limits, extracting Bacs files, contingency arrangements and the responsibilities for the receipt and verification of the Bacs Input reports.	To enhance the existing agreement we recommend it details the specific responsibilities for verifying and addressing any rejected or adjusted records identified in the 'AWACS' (Advice of Wrong account for Automated Credits Service) and 'ARUCS' (Automated Return of Unapplied Credits Service). Recipients of these reports are required to action them no later than three working days from receipt, and inform the beneficiary if the payment has failed. Furthermore, the Service User should establish the correct account information and update their records accordingly.	31st January 2016
Physical security	We assessed the bureau as being **EXCELLENT** in this category.	No findings reported.	No recommendations made.	Not Applicable.

Area	Conclusion	Findings	Recommendation	Implementation date
Computer operations	We assessed the bureau as being **GOOD** in this category.	As Microsoft will cease mainstream support of specific applications, we understand that RCT CBC has embarked upon a project to upgrade existing operating systems.	We endorse this course of action and recommend all server and PC operating systems are upgraded as soon as possible and remain fully supported at all times.	31st March 2016
		In the event of a disaster scenario preventing access to the Bronwydd House offices, Bacs operations could resume from any other Council building given the WAN architecture. Server images including Bacs-related data would be available from the back-up tapes. One PKI smart card, used for the transmission of Bacs data, is held off-site for contingency purposes; however, this does not include a copy of the Bacs smart card software (eSigner).	We recommend a copy of eSigner is stored securely off-site for contingency purposes, along with the PKI smart card and a spare card reader.	31st December 2015

Area	Conclusion	Findings	Recommendation	Implementation date
Computer operations (continued)	We assessed the bureau as being **GOOD** in this category.	We understand there is a schedule of regular off-site restore tests; however this does not include a test submission to the Bacs clearing.	We recommend the recovery plan for Bacs operations is tested on an annual basis including the submission of a test transaction to the Bacs clearing.	29th February 2016
Applications and systems support	We assessed the bureau as being **EXCELLENT** in this category.	No findings reported.	No recommendations made.	Not Applicable.
Bacs processing and operations	We assessed the bureau as being **GOOD** in this category.	The Council currently has 2 Primary Security Contacts (PSC) and 2 Additional Contacts (AC). We understand 1 of the AC's has recently left the employment of the Council.	We recommend the Council removes this person as authorised contact as soon as possible. We further recommend that all PSCs and ACs are reviewed on an annual basis.	Implemented.
		Overall, Bacs operations, including how to deal with rejected and returned items, appear to be well established and controlled. Operational procedures for Pensions/Payroll and Bacs processing have been formally documented with the exception of the procedure recalling Bacs payments.	We recommend the procedure for recalling Bacs payments is formally documented in the operation procedures.	Implemented.

This page intentionally blank