FUJ00082226

CHARTERIS

Subpostmasters v Post Office Limited

Expert report of Dr Robert Worden

Appendices

Draft 44
30 November 2018

Table of Contents

FUJ00082226

CHARTERIS

FUJ00082226

CHARTERIS

Appendix A GLOSSARY OF TERMS

1 The terms used in this report are defined in the table below:

Term	Meaning
APOP	Automated Payment Out-pay Database
APS	Automated Payment Service
BRDB	Branch Database
BTS	Branch Trading Statement
CA	Cash Account
DBMS	Database Management System
DRS	Data Reconciliation Service
DWH	Data Warehouse
HLD	High Level Design
HNG	Horizon New Generation (or Online) implemented in 2010
IS	Infrastructure Services
KEL	Known Error Log
Legacy	The original version of Horizon before HNG
LFS	Logistics Feeder Service
MSC	Managed Service Change
NBSC	Network Business Support Centre
Pathway	ICL division created for Horizon, which later became part of Fujitsu
PCI	Payment Card Industry
POLSAP	To be completed
POS	Point of Sale
RAC	Real (?) Application Cluster
RDDS	Reference Data Delivery Service
RDMC	Reference Data Management Centre
RDMS	Reference Data Management System
SSC	Software Support Centre
SPM	Subpostmaster
TC	Transaction Correction
TES	Transaction Enquiry Service
TPS	Transaction Processing Service
VPN	A Virtual Private Network is a secure channel that appears to be private despite being carried on a public network, typically the Internet.
WSPOS	Web Services POS

FUJ00082226

Appendix B ACCOUNTING SYSTEMS

2 Computerised accounting systems have been in use since the 1950s, and accounting is one of the most mature applications of computers in business. The techniques for building these systems are very mature, as are the safeguards for ensuring that they work correctly. This section is an introductory survey of the practice of building computerised accounting systems, and covers:

- The business requirements that computerised accounting systems must meet
- The different users of accounting systems, and the ways in which they use them
- The checks and safeguards built into accounting systems, in their current architectures
- The levels of trust which business users commonly place in their accounting systems

Appendix C Business Requirements for Accounting Systems

3 Before computerised accounting systems existed, the profitability and financial health of any business enterprise was tracked by a process of manual bookkeeping. In this process, clerks would manually record every financial transaction of the business in books of accounts (or ledgers) which could be inspected to assess the financial health of the business, or to assist in making management decisions. There would be periodic checks of the information in the ledgers, to check two things:

a) that the ledgers record a self-consistent (and therefore possible) state of the business

b) that the state of the business, as recorded in the ledgers, was in full agreement with some external reality (such as physical stock, or bank accounts)

4 Both checks involved arithmetic sums - either of money, or physical assets, or of commitments to pay money or transfer assets. Each check was a check that two different sums, made from the ledgers or as sums of some external quantities, gave the same amount.

5 If either of these checks failed, there would have to be a process of drill-down, of the following form: "sum A is not equal to sum B. We can examine the components of sum A, and the components of sum B, and place them in correspondence with one another, to find out where the discrepancy arises". Having found the source of the discrepancy (and if necessary having taken corrective action in the business) some correction would be inserted in the ledgers, so that after the correction the ledgers again held a consistent and accurate picture of the business - which again would pass the checks (a) and (b).

6 The requirement (b) - that the ledgers should always agree with the external physical reality - has always existed. It has always been the case that the records written in ledgers are a representation of external reality, rather than reality itself. Therefore, changing a record in a ledger does not change external reality. Changing the ledgers does not alter the true financial health of the business, which depends only on external reality, such as its cash and bank accounts and other assets. However, the state of the ledgers should accurately reflect that external reality - and if it does not do so, to the extent that it does not, the ledgers are less useful. The ledgers are intended to track reality as precisely as possible, and to require correction (to match reality) as infrequently as possible -

FUJ00082226

because that is a time-consuming and expensive process, which reduces the confidence of those parties, internal to the business and external to it, who rely on the ledgers to understand the state of the business.

7 The requirement (a) - that the ledgers should present a self-consistent picture of the state of the business - has not always existed. It is possible to keep a set of ledgers as one or more lists of assets and liabilities, with each asset or liability recorded only once, so that no internal check of self-consistency is possible[1]... That changed around the fourteenth century, with the invention of double entry bookkeeping

8 We can understand double entry bookkeeping by starting with the simple case of a trader on a farmer's market, who has some money, and who has some sheep. He can keep a list of his money, and a separate list of his sheep - complete with their names if he wants to. He can track changes to those lists, with entries like '23rd July: sold one sheep - Dolly'. From the changes he can work out his current position, in money or in sheep: 'now I have 17 sheep left'. This is single-entry accounting.

9 Double-entry bookkeeping starts when his list of sheep contains two types of information - the sheep he has, and the price he paid for them; and he also keeps a separate list of his money. He tracks the changes to these lists in a series of dated transactions: '25th July: bought one sheep for 5 shillings'. With that transaction, the sum of his money list goes down by 5 shillings, and the money total of his sheep list goes up by 5 shillings. So, he makes two entries - in those two lists - with money value -5 shillings and +5 shillings, and the total money value of the two lists does not change. Because of the self-consistency of mathematics, however he chooses to do those two sums, the sum of the two sums should not change from day to day. This is his double entry 'trial balance'. If the number does change from any day to the next, he knows he has made a mistake - and he can start to track it down.

10 The basic double entry principle is easily extended to more complex cases - when he sells a sheep for more than he paid for it, and so makes a profit; when he borrows some money and incurs a debt, when he owes some tax, and so on. The basic principle remains. Whenever he makes entries in his books for any type of transaction, however complex, he always makes at least two entries in different columns of figures - and does it in such a way that the net value of all the money entries is zero. Then the sum over all the columns of figures should not change from day to day. That is his self-consistency check on the figures.

11 We need to understand why double entry bookkeeping was such a powerful advance, which swept across Europe within a few years of its invention.

12 Because any accounting system is intended to track external reality, and to give the most accurate possible picture of that reality, it is essential from time to time to check the picture of reality, held in the accounting system, against reality itself - the physical assets of the business, its money in cash or banks, its obligations and debts.

13 However, checking against external reality is (or was) an expensive process. You cannot simply look at the books - you have to get up from your desk, go out into the warehouse and count stock, check your bank balance and count your cash, consult other people, and so on. Because checking against reality was an expensive process,

1 This was the case, for instance, in the clay tablets of accounts found at Ur and Knossos.

FUJ00082226

it did not get done very frequently. If the check is only made occasionally, and mistakes are found, the interval of time in which one or more mistakes might have occurred is a long one. The error is more likely to have arisen from multiple mistakes. Looking for several mistakes together is much harder than looking for one mistake; there is no 'telltale number' to look for. The process of 'drilling down' to find the origin of a mistake is difficult and unguided, with few clues.

14 Double entry bookkeeping changed this. If a bookkeeping mistake is made, that mistake will lead to a discrepancy against external reality, which will eventually be found in the external reality check. But any mistake is most likely to have occurred in one column of figures, without any balancing mistakes on the other columns. So, the mistake will immediately destroy the trial balance. Checking the trial balance is much easier and cheaper than checking against external reality. It can all be done by sitting down at a desk with the books and an abacus or calculator - so it can be done much more frequently. When a discrepancy is found, it is now much easier to drill down and find its cause. For instance, if each entry in the books is dated (as it will be), by just inspecting the books you can find the exact date and nature of the transaction which was not recorded as zero-sum, and which destroyed the balance.

15 So double entry bookkeeping immediately reduces the cost of keeping accurate and trustworthy accounts. It was an early, and highly effective, form of error repellency - in a time when manual errors of bookkeeping were likely to be frequent. The error repellency guarded against a single point of failure (i.e. a mistake in a single column of figures) by making any such mistake rapidly and obviously visible, in the next trial balance.

16 The use of double entry bookkeeping had other important commercial advantages, as well as reducing the costs of keeping accurate books:

- **Working in a network of trade**: From the beginnings of trade, trade consisted of a network of traders, exchanging goods, services and money between them. For any two individuals or parties to trade as part of the network, they have to agree a basis of trading between them (e.g. in a contract) and they need both to monitor that their trading conforms to that agreement (e.g. that I am charging you the price we agreed, and for that price I have delivered to you the goods we agreed). Trade depends on the two parties agreeing what actually occurs between them, down to a very detailed level (which may be down to the last penny). To check this agreement, day by day or month by month, they each use their sets of accounts. Party A looks in his accounts to say: 'on Thursday I delivered to you 5 widgets' while party B looks in his accounts to say, 'On Friday 5 widgets arrived'. Without this agreement they cannot trade.

  Therefore, any set of accounts is repeatedly being checked against several other parties' sets of accounts. Some selected extract from A's accounts is compared with a selected extract from B's accounts, and they should match - both item by item and in monetary sums. Any discrepancies between the two are like sand in the bearings of a machine - they hinder trade, reduce trust, and lead to additional costs. In these circumstances, having the error repellency and increased reliability of double-entry bookkeeping reduces the risk of discrepancies, gives you the means to find the origin of any discrepancy, and gives you a commercial

FUJ00082226

advantage over any competitor or business partner who does not have equally accurate accounts- because you are more reliable and easy to work with.

- **Reduction of fraud and theft**: Any large business is likely to delegate the process of bookkeeping to employees, rather than the owner. These employees see large sums of money passing through the books they keep and may be subject to the temptation to 'skim a little off' for themselves - possibly in small amounts, which they hope will not be noticed. With single entry bookkeeping, this could be a straightforward process. Take a bit of cash and, at the same time, alter the cash ledger so it matches - so that counting the physical cash, and matching it against the books, will show no discrepancy. But with double entry bookkeeping, it is not so simple. If you just alter the cash ledger on its own, without some balancing entry in another ledger, you destroy the trial balance - which will soon be discovered. If you try to be more clever - taking 5 shillings from the cash ledger and adding 5 shillings (the price of one sheep) to the sheep register, that will not be discovered until later, when the sheep are counted - but when it is, the owner may be able to drill down or recall events, to find the exact day on which the discrepancy arose, and who wrote it in the ledger. Alternatively, the owner himself may be tempted to falsify the accounts. Double entry bookkeeping makes this much harder to do, dramatically increasing traceability.
- **Accounting to external parties**: With the growth of capitalism, the typical business was not simply the property of one owner, beholden to nobody else. The accounts were no longer just a tool for that person to manage his own business but were also an essential tool to explain the state of the business to external stakeholders - such as shareholders, banks who lent it money, or governments who taxed it. To say to these people: "you can look at my accounts or audit them, to check the truth of what I tell you about the business", the self-consistency check of double entry accounting became an essential tool - a pre-condition for checking and trust.

Appendix D Discretionary Elements in Accounts

17 A primary use of an accounting system is to enable external stakeholders to understand the state of the business - in the last resort, to understand whether it is a going concern. One of the key metrics to support this understanding is the profitability of the business.

18 In the long term, profitability is a matter of whether a business makes more money than it spends. There is a formula: profit = revenue - expenditure, which every businessman understands. However, in the short term - over the course of one financial year, or even one quarter - it is more complicated than this. Profit is not simply a matter of cash in versus cash out.

19 Put simply, there are peaks and troughs in cash flow, which need to be ironed out to understand the true state of the business. One of the simplest examples is the use of a capital asset, such as a computer. The business needs to buy a new computer every five years, and that is expensive. But once done, there is no further purchase needed for another five years. The profitability of the business should not be depressed once every five years, when it needs to buy a computer.

FUJ00082226

20 Conventions of accounting have been developed, which allow a company's accounts to reflect this reality. The company can 'capitalise' the cost or the computer - so it does not depress profit during the year it is bought - and 'depreciate' that cost uniformly over five years, so that it appears as a uniform cost and depresses profit uniformly over that period. The long-term effect on cumulative profit is neutral. This convention is intended to provide a more realistic picture of the fortunes of the company in each year. But it does introduce an element of management discretion, over which kinds of expenditure are capitalised; and that discretion might be misused for short-term purposes - such as to inflate profits in one year, to attract investors.

21 Other elements of management discretion introduce more subjectivity. For instance, if a company invests some of its resources (money, physical assets, people) in developing a new product, which it hopes to sell profitably over a period of several years, then it may be able to capitalise that investment in the expectation of the profit it will bring later. As before, the long-term effect on cumulative profit is neutral; but year-on-year figures are altered.

22 Other discretionary elements include debtors (where the management needs to assess: how likely they are to pay) and legal disputes (how much money should be set aside in the accounts against an unfavourable outcome?). In all these cases, management discretion affects which accounting period (year or quarter) the profit appears in but does not impact the long-term cumulative profit.

23 All accounting systems, manual or computerised, need to be able to have areas in the accounts where these discretionary management assessments of the business can be recorded, and can be assessed by external stakeholders (such as auditors, acting for shareholders or the taxman) to test whether the assessments can be justified.

24 It is our current opinion that any discretionary elements of the Post Office accounts are not related to the Horizon dispute. The Post Office's business relationships, both with subpostmasters acting as its agents, and with its 'client' organisations such as DVLA, banks or Camelot, all involve flows of cash or assets whose relation to profit is direct and short-term, not involving the management assessments and transient adjustments of the kind we have described above. We have included this discussion in case any discretionary element of PO accounts becomes relevant to the Horizon trial.

Appendix E The Users of Accounting Systems

25 From the above it will be evident that information in an accounting system may be of interest to several diverse groups of people, in and around a business. With the onset of Enterprise Resource Planning systems (ERP systems) in the 1990s, which include an accounting system and much other functionality, the scope of accounting systems was widened to include many business functions (such as manufacturing and human resources, sales and service delivery) not within the scope of a pure accounting system. For organisations, which use ERP systems (such as SAP), the line between users of the accounting functionality and users of the other functionality of the ERP system is blurred. Even if a company uses a pure accounting system (which it typically needs to integrate with other business applications), there are several different classes of user of the accounting system.

FUJ00082226

26 We first distinguish two main classes of use of an accounting system. An accounting system may be used to provide information to the managers of the business - to help them make decisions about how to manage the business - or it may provide information to external stakeholders such as shareholders or government departments (such as taxation departments) who have a right to information about the business. In the former case, it is known as a management accounting system. In the latter case, it is a financial accounting system. The distinction between the two is by no means clear-cut, in that some accounting systems provide parts of both types of functionality and the information required for the two functions has a high degree of overlap.

27 Users of financial accounting functionality include:

- The corporate finance department
- Senior management, when inputting the discretionary elements of the accounts (often through the finance department)
- External auditors

28 Users of management accounting functionality include:

- Staff in business departments who input the information used by the system (where that information is not automatically generated)
- Managers of 'vertical' slices of the business (such as all PO business with Camelot)
- Managers of 'horizontal' slices of the business (such as a region or branch)
- External auditors

29 Typically, the full scope of management accounts and financial accounts is within scope of an external audit, such as an annual audit of accounts. Thus, auditors need to access both kinds of information.

30 We understand that the financial accounting functionality for the Post Office was provided by SAP over most of the disputed period (from 2004 by POL FS, a SAP application, which in 2010 merged with SAP ADS to form POL SAP), whereas Horizon provided mainly management accounting functionality, as well as Point of Sale functions for the branches. This dual nature required close integration between Horizon and the SAP systems, so that pictures of financial reality given by the two systems were at all times mutually consistent. There is a large overlap between the information stored in the two systems, which will be described below.

Appendix F Functionality of Computerised Accounting Systems

31 The functionality of a computerised accounting system includes the following:

- To securely store detailed information about all the assets and liabilities of the company, in a set of accounts, defined by account codes (in the company's chart of accounts)
- To provide facilities for the input and checking of that information, either manually or from other computer systems
- To ensure that the information is always self-consistent, according to the criteria of double entry bookkeeping

FUJ00082226

- To provide highly flexible output and reporting functionality, which includes:
  - Summations of items to verify the self-consistency of the data
  - The information required in the annual accounts of the business
  - Extracts of the information concerning all transactions made with some external business entity during a period (e.g. the information required to bill that entity, or to pay that entity)
  - Extracts of the information relating to all the activities of any internal sub-unit of the business during a period (e.g. a division, or an individual branch), typically used by line managers who have responsibility for some part of the business
  - Miscellaneous other slices of information, for diverse purposes (e.g. personnel management), typically used by staff managers who have responsibility for some aspect of the business.
  - Many kinds of 'drill-down' and aggregation to inspect individual items in the accounts, or small selected groups of items - for instance, to investigate anomalies

32 Most other functionality consists of extra functions provided by particular accounting systems, rather than by accounting systems in general.

33 From this, it is evident that the functions of an accounting system include the input, secure storage and output of many types of information, in large volumes (many transactions per day), with rather little computation. By far the most important type of computation that occurs in financial accounting is straightforward summation of numerical quantities such as money and stock, subject to the rules of double entry bookkeeping. For management accounting, some other kinds of computation are needed - for instance, for forecasting purposes; but they are usually not computationally demanding or complex.

34 It would be difficult to exaggerate the diversity and flexibility of the reporting and drill-down functionality required of an accounting system. Any person in any management capacity in the business has, through their own particular role, a point of view and a focus of interest about the many transactions done by the business - and that person may require selected 'slices' of information from the accounting system, tailored and aggregated to the appropriate level for his or her interests. This makes for a substantial number of information slices that may be required from the system. Fortunately, modern computer technology has highly flexible and easily configurable ways of meeting these reporting requirements.

Appendix G The Architecture of Accounting Systems - Relational Databases

35 Although computerised accounting systems have been in widespread use since the 1960s, there was a major step change in their architecture in the 1980s, with the advent of relational databases such as Oracle. Hence, it is only necessary to describe the architecture of accounting systems which, like Horizon or SAP or almost every other accounting system now in use, are built on relational databases.

36 The database of an accounting system is managed by a piece of system software called a Relational Database Management System (RDBMS, or DBMS). This is built and supported not by the accounting system developer,

FUJ00082226

but by a supplier of system software, such as Microsoft or Oracle. The accounting software makes calls to the RDBMS to store and retrieve the information.

37 The technology of relational databases matured during the 1980s, and most RDBMS date from that era. They are now very mature, stable and feature-rich products. As they are the essential foundation of accounting systems, it is necessary to say a little here about how they work.

38 The information stored in any computer system can be broadly divided into two types: structured information, and unstructured information.

39 The commonest examples of unstructured information are free text, or pictures, or video clips - of which there are vast amounts in resources such as Facebook or YouTube. There may be some structure which is discernible to a person in a passage of text or an image, but it is not the kind of obvious structure which can be used by a simple computer program. For a computer program to understand and use that kind of structure, it needs to be a very advanced computer program, using techniques of Artificial Intelligence (AI). This is well outside the scope of accounting systems, which use structured information.

40 Two familiar examples of structured information are:

- A spreadsheet
- A bank statement

41 The structure of these is visible in the rows and columns. Each column of a spreadsheet contains only one type of information (such as a number, or a monetary amount, or a date, or a code). Each row of the spreadsheet contains a set of column values (in the 'cells' of the row), which are linked to one another as a single item. The different cells in one row contains different pieces of information about one item.

42 Because of this easily discernible structure, simple computer programs (using no AI) can make use of the information - for instance, summing all the values in one column.

43 While a relational database can sometimes be used to store unstructured information, the main use of a relational database is to securely store large volumes of structured information. The way it does so can be understood as having large numbers (tens or hundreds) of different spreadsheets (which are called tables) and which are linked to one another. Two different tables in a database are linked to one another (in a 'relation') when they both have one or more columns with the same meaning and share values in those columns.

44 A typical relational database may have tens or hundreds of separate tables; each table may have tens or occasionally hundreds of columns; and a table can have any number of rows, up to millions if necessary.

45 One relational database can act as a 'server' to one or more application programs, which are performing actions directly visible to their users. The application programs make calls (requests) to the relational database management system, which alters or retrieves the data to fulfil the requests. The core service provided by the relational database is to securely store and retrieve this information, for the application programs, or for others who retrieve information from the database more directly. Both the phrases 'securely store' and 'retrieve' have a lot packed into them.

FUJ00082226

46 The phrase 'securely store' implies several guarantees: that once an item of information has been stored in the database, it will not be lost or unintentionally changed; and that it is a part of a consistent collection of information, whose integrity will not be compromised in any way.

47 The idea of integrity of information is central to relational databases. When the structure (tables and columns) of a relational database is first defined (in a relational schema) that schema defines various types of integrity constraint on the data, for instance that:

- certain columns in tables are mandatory, and will always be given values
- There can never be a record in some table (call it table A) unless there is a corresponding record in some other table B. For instance, there can never be a record of an invoice to a customer, unless a record exists for the same customer. The invoice table and the customer table both have a column 'customer id'; for every invoice record, there must be a customer record with the same customer id.

48 The database management system guarantees that these integrity constraints will be true for all time. If any application tries to make a change to the database which would violate an integrity constraint, that change is rejected by the DBMS, and no change is made at all. One change to the database may involve changes to several tables at once, so that after all the changes are made, the integrity constraints are still true; but part way through the changes, the constraints are temporarily untrue. One such package of changes, involving changes to one or more tables, is called a database 'transaction'. The DBMS guarantees that:

- After any completed transaction, the database will still obey all its integrity constraints.
- After any completed transaction, the changes made to the database can never be lost - even in the event of hardware failures; there are robust ways to recover the information.
- If a transaction would violate an integrity constraint, it is not allowed by the DBMS; no changes will be made to any table, so the database will still be in a consistent state, as if the change had never been requested.
- When one application is making multiple changes to the database in a transaction, so that the database is temporarily in an inconsistent state (when some but not all of the changes have been made), those changes are never visible to other applications or users before they have all been completed. Other applications and users can only ever see a consistent state of the database (either before all the changes, or after all changes), in which all the integrity constraints are true.

49 This set of guarantees, given by the DBMS, is called 'transactional integrity'. It has been built into the fabric of all relational databases and has been relied upon by thousands of applications which use relational databases, since the 1980s. Builders of applications can have a very high degree of confidence that their DBMS will maintain transactional integrity. Builders of accounting systems have relied on that guarantee.

50 Selective retrieval and reporting of records is a fundamental capability of all relational databases. All relational databases support the language SQL (Structured Query Language), which can be used from within application programs to retrieve typically small numbers of records from a few linked tables, filtering the records based on

FUJ00082226

the data values in their columns. SQL is a powerful language, enabling an application to pick out from a large database just the few records it is concerned with at any time. The DBMS supports these operations very efficiently, using fast indexed searches rather than brute force inspection of all the records in a table.

51 SQL can be used directly by end users, without the use of any application program, to selectively retrieve and display records. However, it is more common for the users to use a general report writing tool, which not only retrieves the required records, but formats the information in easy-to-read reports - with appropriate column headers, formatting of fields, grouping of records, computations of sums of groups of records, and so on. Nearly all the reports needed from an accounting system are created using these report writing products, which can be rapidly configured to produce any new kind of report, either one-off or regularly as required.

52 All these capabilities of a relational database have been present in relational database products such as Oracle since the 1980s and have been tested by possibly millions of different applications which use those capabilities and rely on them. So, when we are discussing the issue of bugs in an application such as Horizon, the possibility that these bugs arise from bugs in the underlying DBMS - particularly when it is the world market leader Oracle - is extremely remote, and we shall ignore it.

Appendix H How Accounting Systems Use Relational Databases

53 Comparing the core functionality of an accounting system - which is to store and retrieve accounting data - with the functionality of relational databases - which is to securely store and retrieve any kind of structured data - there is a large overlap between them. For many of its required functions, an accounting application program uses the underlying features of the relational database.

54 Therefore, essentially all contemporary accounting systems are built using a relational database, whose database schema has been designed to hold accounting data; and an accounting application program which makes updates to the database, subject to the rules of double entry accounting; and a set of reporting and retrieval functions which are built using the reporting and retrieval functions of the RDBMS.

55 Accounting systems use their underlying database to store information redundantly, so that the effects of each accounting transaction are typically stored in several different forms, in different tables of the database. For instance:

- There is usually some kind of message log, which stores each transaction in its 'incoming' form.
- The accounting information derived from each transaction is stored in both a General Ledger - which holds summary information about all transactions - and several more specific ledgers, which typically hold information at a more detailed level.
- Information is stored in other tables for audit purposes.

56 Given these redundant forms of storing the same information, it is possible to make many checks of the mutual consistency of the different forms. These checks are discussed in the next section.

57 Accounting systems are used by many different types of organisation, which need to track and organise their business in specific ways. To track money and resources in the way best suited to manage its business, each

FUJ00082226

organisation typically has its own chart of accounts, defining a set of account codes, under which all its transactions are accounted for. Each organisation has its own set of rules for allocating income and outgoings to particular account codes.

58 If the accounting application software was written in a way that depended directly on the chart of accounts, then each company would need different accounting software. This would be very uneconomical (in writing and testing all that software), and it is not done that way. The chart of accounts is not 'hard coded' into the application software. The software is written to work with any valid chart of accounts; and the chart of accounts itself is treated as data, stored in the database. In this way, changes in the chart of accounts (which occur from time to time) do not require changes in the accounting software.

59 This is one example of data-driven software - in which any requirement which might change frequently is encoded as data, rather than software code. The code is written and tested to work with all allowed values of the data, to meet a wide range of requirements by changing the data rather than the code. The modern practice of software engineering is to use data-driven software as far as possible. This is not always as far as one might like; some differences between companies and their requirements are best expressed as differences in code, rather than data.

60 Building an accounting application 'on top of' a relational database is one example of a layered software architecture. Most accounting systems, including Horizon, have a layered architecture. At a minimum, three layers are usually found:

- A user interface layer, responsible for presenting information to users, and accepting their inputs
- A business logic layer, responsible for carrying out business processes, and supporting users in doing so
- A data layer, responsible for storing and retrieving data.

61 Most software architectures are more complex than this, with more layers, or with layers within layers. The practice of object-oriented software development, which is now almost universally used for building software applications, encourages the use of many layers.

62 In a pure accounting system, the role of the business logic layer is comparatively simple - in that it does not involve long or complex sequences of business operations. Complex business processes are either manual or are done by other applications. When updating the accounts, the main role of the accounting business logic layer is to accept business transactions, ensuring that they obey the laws of double entry accounting, as reflected in the chart of accounts for the business. Every incoming business transaction is classified as one of several allowed types of transaction. According to the type of transaction, the items within the transaction are mapped onto account codes in the chart of accounts, in a way conformant with the laws of double entry bookkeeping and are passed to the data layer for storage - usually for redundant storage, including for instance audit information.

63 Similarly, for the retrieval and use of the accounting information, the role of the accounting business logic layer is in principle simple, compared to some other applications. Much of the business logic consists of selecting and arranging information that is useful to users such as line managers or the finance department. This is typically

FUJ00082226

done using data-driven report writing software, rather than bespoke application code. The other role of the business logic layer is to carry out many kinds of check, both internal and external, on the accounting data. These checks include the trial balances of double entry bookkeeping.

64 The user interface layer of an accounting system includes the many reports it can produce, and typically includes a modern Graphical User Interface (GUI) used for a wide range of purposes. In the case of Horizon, the user interface also includes a Point of Sale interface, for use in Post Office branches. This interface is best thought of as part of the Horizon Point of Sale application, rather than the Horizon accounting application.

Appendix I Checks Built into Accounting Systems

65 Computerised accounting systems are perhaps the most widely used type of computer application in business and are also the most widely relied upon. It is therefore an essential requirement that they should build in sufficient checks on their working to justify this reliance. The following sub-sections illustrate these checks.

Appendix J The Double Entry Check, and Other Accounting Equations

66 We first illustrate, in a simplified example, the basic check built into all double entry bookkeeping systems. Suppose the chart of accounts of a company includes, amongst others, two ledgers - a cash ledger, listing various holdings of cash held by the company, and an accounts receivable ledger, listing amounts of money owed to the company by its customers.

67 An initial snapshot of these two ledgers is shown in the table below:

	cash	accounts receivable	sum
	30	100	
	50	20	
	10	15	
		30	
sum	90	165	255

Table B.7 .1 – Double entry example

68 In practice, each of these ledgers would hold more information. For instance, the accounts receivable ledger would list the identity of the customer who owed each sum of money, the date on which it was due, and so on. They would also typically have many more entries. These details have been left out for simplicity. Each ledger is just a list of items, with no necessary link between the two columns. The fact that some 'cash' item appears in the same row of the table as some 'accounts receivable' item is just an artefact of this simple table and has no significance. The sums at the bottom, as can be verified, are simple arithmetic sums of the columns.

69 Now suppose that the customer who owes £20 pays off £11 of his debt. These £11 are added to the holding of cash which was previously £10, giving £21; and, at the same time, they are subtracted from that customer's outstanding debt of £20, leaving £9. This leaves the ledgers in the state:

FUJ00082226

	cash	accounts receivable	sum
	30	100	
	50	9	
	21	15	
		30	
sum	101	154	255

Table B.7 .2 - Double entry example

70 Therefore, the sum of each ledger column is altered - but the sum of the two sums (£255) is not altered. This is because £11 has been added to it, and at the same time £11 has been taken away.

71 The constancy of the sum £255 is the fundamental check of double entry bookkeeping. It can be made at any time, in a trial balance.

72 The double entry check is just one of many accounting equations, in which two separately derived sums must be exactly equal at any time - and therefore the changes to those sums in any time period must also balance. The check is only a check because the data are stored redundantly - with at least two accounting entries for each business transaction. It would be possible not to store the data redundantly, but to calculate each of the matching figures from non-redundant data, in a way that would guarantee their equality. However, that would be single entry accounting, and is no longer done.

73 Similarly, for many other accounting equations, where two figures should always be equal, it would be possible to store the data without redundancy and to compute the figures in a way that was guaranteed to match. That would not be a check on the data. In practice, however, accounting systems store data with a high degree of redundancy so that the checks are meaningful and will detect an error in any one of the redundant data items.

74 This redundant data storage increases the number of independent data items which would need to be altered in a coordinated manner - for instance, by a bug in the software, or by fraudulent activity - to make some change which was not detected by the arithmetic checks.

Appendix K Checks on Data Entry, Including Double Entry Checks

75 We note various aspects of how double entry bookkeeping is implemented in a computerised accounting system, and the checks that are built in:

- In practice, a company's chart of accounts will contain many different account codes (such as for the two ledgers above), and the company will have rules for how each type of business transaction is to be allocated across different account codes. These rules will all respect the rules of double entry accounting, in that each business transaction of any kind must be 'zero sum' in its net effect on all accounts (as seen in the general ledger, when it is balanced).
- In the example above, the item in 'accounts receivable' which changed from £20 to £9 does not have a single date, because it is composed of at least two separate events (the incurring of the debt and paying off

FUJ00082226

a part of it). There is usually some more detailed ledger in which every item is dated, and there is a separate consistency check between the more detailed ledger and the accounts receivable ledger shown here.

- If a discrepancy in the trial balance were to arise, it would be possible to drill down to the most detailed ledgers of time-stamped items to find out exactly when and how it arose. However, other checks in the software make it extremely unlikely to have arisen.
- In a layered software architecture, with a business logic layer and a data layer, there would be double entry bookkeeping checks in both layers. In the business layer, every business transaction could only be packaged up into a set of related postings to accounts (in Horizon's case, a basket) which had zero net effect on all accounts. In the data layer, the software directly above the RDBMS would only accept packages of updates with zero sum and would reject any other package. This practice is known as 'defensive programming' - where the different parts of the software architecture are each built defensively, to protect themselves against possible errors in other parts.
- In this respect, the periodic trial balance of the general ledger is the third line of defence against accounting errors.
- Once a package of updates has been passed to the RDBMS, it may involve several different updates to different ledgers, whose net effect does not alter the balance, but which do alter the balance temporarily when only some of the updates have been done. The transactional integrity of the database guarantees that either all the updates will succeed (so that all of them are securely stored, with no net effect on the balance); or none of the updates will succeed, again with no net effect on the balance. In the latter case, the user will be warned of the failure, and may need to redo some work.
- The database also guarantees that while a sequence of updates is being done for one of its client applications (e.g. for one branch) - so that the database is temporarily an unbalanced state - that unbalanced state is not visible to any other client application. At any time, all client applications can see only a consistent, balanced state of the database.
- Once accepted, any update to the accounts is guaranteed to be secure and recoverable against nearly all possible hardware errors - certainly it is guaranteed against any single point of failure.

76 The net effect of these measures is a powerful form of error repellency, in the following sense: each business transaction is split into several different postings to the accounts, which obey the double entry zero-sum constraint. This package of updates is created in the business logic layer, is checked to be zero sum in that layer and is delivered to the data layer - where it is checked again. Then the different updates in that business transaction are 'scattered' by the DBMS to many different parts of the accounts - to different tables and rows in the database - and are redundantly copied to other parts of the database. From that point onward, any software error, which could lead to an erroneous computation from any one of those elements, is most unlikely to lead also to a compensating error in the other elements, in other parts of the database. This would be like lightning striking twice, in two precisely coordinated ways -which is vanishingly unlikely. Therefore, any such software

FUJ00082226

error will lead to an error in the trial balance - and it will probably do so frequently. Such an error is very easy to detect.

77 An error in the trial balance is the most serious kind of error in an accounting system. Any such bug should be found and fixed in testing, or at least very early in the service life of the software. So, it could not persist over a long service life.

Appendix L Checks in Retrieval and Reporting

78 The trial balance is by no means the only check which applies to an accounting system. The many forms of redundancy built into an accounting database (for instance, between detail accounts and summary accounts, which must tell the same story) all lead to consistency checks - which can be made either automatically in the software, or manually by users, by comparing numbers in different reports from the system. These are all checks in the self-consistency of the data, and many kinds of software bug would lead rapidly to violations of these checks - so the bugs would be quickly detectable and would need to be fixed immediately.

79 The reporting tools used with accounting systems have powerful facilities to 'slice and dice' the data - to produce many different selective subsets of the data, which are vital daily information for many managers. The managers closely inspect these reports, and then 'drill down' and cross-check to find the origin of interesting or suspicious figures. These cross-checks are a part of regular management activity and include both internal and external audit. This constant inspection by many pairs of eyes will soon reveal any software bug which systematically distorts the figures. The accounts matter too much, and matter to too many people, for them to be allowed to be systematically wrong.

80 Some important examples of the cross checks include:

- **Hierarchical comparisons**: Many large organisations have a hierarchical structure of business units and sub-units (such as divisions, regions, and groups) with managers at each level. Data from the accounting system is a vital tool for the management of this structure, in dialogues between line managers and their supervising managers. This requires hierarchical breakdowns of the figures by business unit, with the figures for each unit being the sum of figures for its constituent units. These figures are the subject of intensive discussions between line managers, and they are often linked to personal remuneration, as incentives. Any inaccuracies in the figures arising from software bugs would be rapidly detected and loudly complained about.
- **Time-slice comparisons**: At any level in the line management hierarchy, managers are expected to understand the time dependency of their financial results - how the full year figures break down into monthly figures, and so on. They rely on various accounting systems to provide all this data and scrutinise their outputs carefully. As a simple example, weekly time-slices of figures may be compared against monthly time slices of the same figures, taken from the same database or from a different database. If the sums do not add up (if a monthly sum does not match the sum of its weekly sums, including part-weeks) questions will be asked. Any underlying software error would be rapidly exposed.

FUJ00082226

- **Functional slices of the business**: Overlaid on the hierarchy of business units and sub-units may be another functional structure of specialist skills or cost centres such as human resources, marketing, distribution, manufacturing or R&D. This structure has its own management with financial targets and responsibilities. All those 'staff' managers need reports from the accounting system showing the financial performance of their cost centres, over time and in other dimensions. The managers regard controlling these figures as the essence of their jobs, and the figures may be linked to their remuneration, so the figures are all closely watched.
- **Forecast versus actual comparisons**: Any business is required to look ahead rather than backwards, and managers are required to produce plans and forecasts for the business units under their control. All these plans and forecasts are stored in the management accounting system, and their comparison against actual performance is a subject of keen management interest. These comparisons occur through a wide range of reports from the accounting system.
- **Audit checks**: Audits may be carried out for a variety of purposes - external audit for shareholder, regulatory or taxation purposes; internal audits of performance, or audits to detect fraud. For all these purposes, the accounting systems are required to hold extra (redundant) copies of financial information, and comparisons with the extra information are a central part of the audit process. Financial fraud may involve skimming off money in tiny amounts, so these audits must involve very precise comparisons.

81 In summary, diverse types and summations of figures from an accounting system are carefully scrutinised by many people on every working day of the year. If there were systematic errors in the figures from software bugs, these errors would be rapidly noticed, and the bugs would need to be corrected. That is one reason why accounting systems are highly reliable.

Appendix M External Checks with Other Organisations

82 So far, we have addressed mainly internal checks, within the organisation, of the consistency and accuracy of its own accounts. There is another important class of checks, which are made between organisations - and are just as unforgiving of any software bugs which would distort the financial picture.

83 Whenever two companies do business together, they need to agree what has been transacted between them - for instance, what goods have been supplied, and what money has been paid. A failure to agree these facts is a serious breakdown of a business relationship, and potentially a breakdown of trust. So, it is important to avoid it whenever possible.

84 In order to know the facts of what has occurred between two businesses, each business relies on its own accounting systems. It does not necessarily trust the other business's accounting systems. For instance, to issue an invoice, company A looks at its own accounting system. To know if an invoice has been paid, company B looks at its own accounting system. A can continue to do business with B only if these two versions of the facts are in agreement. Therefore, the managers involved, in both businesses have a keen interest in knowing that they agree, and in avoiding unnecessary misunderstandings - which would consume management time and reduce

FUJ00082226

trust. The processes for comparing these two versions of the truth, and detecting possible discrepancies, are in all but the simplest cases automated using the accounting systems or data extracted from them.

85 Therefore, for most large businesses, their accounting systems are required to make selective retrievals of the accounts- extracting all the data about their business transactions with some other business - and to compare that data with a corresponding set of data from the other business. Possibly the comparison is made by other applications, using data extracted from the accounting systems. This process of reconciliation, between the versions of truth held by two independent accounting systems, is a powerful check on the accuracy of both versions. Any discrepancy must arise through an error by one or the other party, and it is in both of their interests to find out where the discrepancy arises and correct it as soon as possible.

86 This places an extra premium on accuracy and lack of bugs in both accounting systems. Any bug in either system, which distorted the financial picture of what had occurred between them, would typically lead to repeated discrepancies which, in the absence of any other account for them, would need to be diagnosed and the bug rapidly fixed.

87 This consideration extends a point which we have made previously - that the purpose of an accounting system is to track external reality as accurately as possible, rather than to change it. The true health of the business depends on external reality, outside its accounting system - such as cash, obligations and physical stock - rather than on the contents of its accounting system. Now, however, we must extend the idea of external reality, to include the accounting systems of other businesses that it trades with. In modern financial networks, financial reality is defined by a network of computer applications, and a network of trust which they embody.

Appendix N Traceability

88 One of the purposes of an accounting system is to detect financial anomalies; and they have a variety of means, including very flexible reporting and cross-checking. for doing so.

89 As soon as any anomaly is detected - which can be as simple as a figure in some report that a manager does not understand, because it looks too high or too low - it is important to be able to understand the origin of the anomaly. So accounting systems have powerful facilities to drill down, decomposing any figure down to its constituent parts, if necessary, down to individual business transactions.

90 Having drilled down to an individual transaction, which may have caused an anomaly in whole or in part, it may be important to answer the question: who or what was responsible for that transaction? This might be a person within the organisation, or an IT system within the organisation, or even some data from a partner organisation. In all these cases, it is essential to be able to trace every business transaction to its originator.

91 Therefore, accounting systems need the means to identify and authenticate every user, and to record the user who initiated each transaction. This usually leads to more redundant copies of data, and more possible cross-checks between them. The need to identify and authenticate users is a necessary protection against fraud.

Appendix O Errors Impacting Financial Performance

92 We have so far discussed the general potential for errors in financial data, including errors arising from software bugs. A conclusion of this discussion has been that many classes of software bug would lead to widespread

FUJ00082226

discrepancies in comparisons and in tests with known results, such as the trial balance of double entry bookkeeping. The consequences of these software bugs would be very obvious and intolerable, so they could not last long in the service life of any accounting system.

93 We next discuss errors which are subtler in effect, and do not trigger a rapid alarm such as a failure to balance the accounts. Are there some of these errors which can alter the apparent financial performance of the organisation or parts of it?

94 We say the 'apparent' financial performance, because the actual performance of a business is not defined by numbers in its accounting system - but is defined by external reality such as physical cash and stock, and bank accounts. The purpose of an accounting system is to track that external reality as accurately as possible, using periodic checks (reconciliation) against all types of external reality, to ensure that the tracking remains as close as possible - and does not drift away from reality through a series of errors.

95 If some input error introduces an inaccuracy in the accounting system, that is usually only a temporary inaccuracy. Some later checking process will discover the inaccuracy, and it will need to be corrected.

96 So, for instance, there are many types of erroneous input to an accounting system which can lead to a transient over-statement of profit. When the error is discovered and corrected, there will be a related transient depression of profit, leading to an accurate cumulative profit after the correction.

97 Similar transient effects can apply to any item of the accounts, such as a cash holding. If some collection of cash is mis-counted in one month; this will lead to an inflated estimate of the cash in hand; but an accurate count in the next month will correct the error, with zero long-term effect.

98 These are errors arising from erroneous input to the system, which naturally obey the principle 'garbage in, garbage out'. It is important to note that although the input is erroneous, it still obeys the principles of double entry accounting, because the accounting software forces it to do so. A balancing double entry is made, but it is an incorrect balancing entry. So, it does not trigger a failure to balance, or any such major alarm.

99 What, then, is the potential for software errors (bugs) which distort the financial performance (even in a transient manner), but do not trigger major alarms such as a failure to balance?

100 In a layered software architecture, there is potential for this kind of bug in the user interface layer. If the user interface displays a cash amount of £3000, while erroneously storing internally a cash amount of £300, and passing £300 to the business logic layer, then:

101 The user will think the transaction involves an amount of £3000 (whether that amount is a consequence of his typing it in, or of some automated data capture), and will approve the transaction on that basis.

102 The effect on the business logic layer would be exactly as if as if the user had made a mistake, entering £300 rather than £3000.

103 This error will get passed on, in double entry, to the data layer and to further retrieval and reporting software.

104 After this error occurs, it could only be corrected by some later checking process - which will inevitably be done. For instance, if the £300 represented a cash amount, later counting of the cash would reveal a discrepancy of

FUJ00082226

£2700. Or if the £300 was a cheque, clearing of the cheque by the bank would reveal the same discrepancy. Whatever the checking process, the net effect would be a temporary upward bump in assets recorded in the accounting system, followed by a later correction to the accurate figure. Because of the checking, the effects of the software error would be transient.

105 Software bugs in the user interface layer have an effect very similar to a user error - causing a transient inaccuracy in the apparent financial performance, which is later corrected.

106 Similarly, there is the potential for software errors in the business logic layer - but mainly only up to the point where the business transaction is split into a set of double entry accounting postings, with zero sum.

107 Up to that point, there is potential for a bug in the business logic layer which converts £300 into £3000. But as soon as the transaction is split into two or more pieces - with £300 going to one account code, and -£300 going to another account code, then it becomes very unlikely for there to be a software bug which converts the £300 to £3000 and makes the same change of -£300 to -£30002. Nearly all software bugs after the splitting into a double entry set of postings would destroy the zero sum, and so the transaction would be immediately rejected - leading to a rapid investigation of the cause of the bug.

108 There is also a further check in the business logic layer. The business logic layer 'dismantles' each business transaction into a set of double entry postings to different accounts. The ways in which it can do so are constrained by the chart of accounts. This chart is defined in data - not in code - so the splitting of the business transaction is almost always defined in data, which drives generic code for all business transactions. The chances of bugs in the generic business logic code are quite remote, since it is exercised and tested by all business transactions. Similarly, the chances of errors in the data defining how each type of transaction is split are remote - because that data is compact and is subject to simple static checking that it obeys the zero-sum accounting constraints; and any other error in the data would lead to robust and reproducible errors for that type of transaction, which would soon be detected in testing.

109 Again, however, even a bug in the business logic layer could only lead to a transient error in the recording of financial performance. Just as for a bug in the user interface layer, some later checking would inevitably take place, leading to a correction.

110 The chances of an error in the data layer which distorted financial performance, and was not rapidly detected, are even more remote.

111 First, the data layer defensively checks any package of postings to accounts, to test if it obeys the zero-sum constraint - and rejects it if it does not.

112 Then, it scatters the different postings to separate parts of the database, with almost nothing to link those postings to one another except their timestamp. The chances of any software error which systematically distorted all these figures, in such a way as not to destroy the trial balance and trigger several other alarms, are very remote. This is not least because the DBMS software has been continually tested by many thousands of applications which rely on it.

2 This kind of bug is very unlikely, but not impossible.

FUJ00082226

113 Next, DBMS software has matured to the point that it offers strong guarantees - for instance, that once a transaction is committed, no data in it will ever be lost.

114 Finally, the data layer makes redundant copies of the data in many different formats - for instance, in a message log of each transaction, and in special forms for audit, and for recovery from hardware failures. There are subsequent tests of the consistency between these forms.

115 Therefore, the chances of bugs in the data layer introducing even transient distortions of financial performance are very small.

116 Finally, we consider the output parts of the accounting system, on the 'other side' of the data layer. Much of this part consists of generic, data-driven reporting tools, which, like the DBMS itself, are relied upon and tested daily by a vast range of organisations, and so are unlikely to have any serious bugs. Configuring these tools is straightforward - much simpler than coding - and any faulty setting up of the tools will soon be detected by users. The rest of the accounting software on the output side, the part which does need to be coded - is specifically designed for automated checking of consistency. This software could in principle have two kinds of bug:

117 bugs which find a discrepancy where there is none (false positives)

118 bugs which fail to find an actual discrepancy (false negatives)

119 Bugs of the first kind are very easy to find and correct; they will 'leap out of the page'. Even modest amounts of well-designed testing will find the second kind of bug, by 'planting' discrepancies which the software should find. In conclusion, software for checking is easy to test, and after testing, is unlikely to have serious bugs. If it did, its users would soon detect them.

FUJ00082226

Appendix P HARDWARE AND SOFTWARE RESILIENCE

120 This appendix provides additional information to supplement section 6.5 of the report.

Appendix Q Branch Hardware

121 Each branch uses a standard PC at each counter. These PCs run the software that provides Horizon functionality to the SPMR and their staff.

122 Many branches have more than one counter and the failure of one (for example through equipment malfunction or loss of power) does not prevent the use of other counter systems.

123 In the original Horizon system, PCs installed in branches with just one counter were fitted with exchangeable hard disk units, as well as fixed disks. If the PC failed, the information held on the external storage could be moved to a replacement PC.

124 These are examples of reliable and redundant hardware (RHW).

125 Each PC is equipped with peripherals such as a touch screen, a customised keyboard, bar code reader and printer. Peripherals can be replaced more easily than the PC itself. Workarounds are also available for many of the devices:

- Keyboard - many transactions are driven entirely from the touch screen or other peripherals and require no use of the keyboard. The software can display a simplified 'soft' keyboard. The clerk can touch the relevant area on the screen to simulate pressing the associated key.
- Bar code reader - all transactions that use data from the reader also allow it to be manually entered by the clerk.
- Printer – the PC software includes a 'print preview' facility for all reports including receipts. The clerk can use this and then copy the screen contents manually onto paper. This is a slow process, but it does provide fallback if necessary.

126 The hardware failure most likely to have an impact on branch accounts is the loss of a PC. This loss may be temporary, in which case the PC is simply restarted. All the data that had been secured prior to the failure remains available for use.

127 In the original Horizon system, important data was stored locally on each counter's PC. Using the Riposte software (described above), this data was replicated across counters - to the exchangeable disk in a single counter's PC - and to the Correspondence Servers in the Horizon data centre.

128 If a PC could not be restarted and was replaced, the data needed to continue trading was retrieved from one of the replicated copies. In this way, the new PC could continue where the old one left off.

129 On HNG, all the important data for each counter is secured centrally. Therefore, a replacement PC simply connects to the data centre and continues as if the previous PC had been restarted (e.g. establishing the working data storage needed to service customer transactions and support the rest of the branch's business operations).

FUJ00082226

130 The procedures for recovery from PC failures depend on the user. If they are in any doubt as to whether a transaction has been completed to the failure, they can use the transaction logs to confirm the position before taking any further actions. If any transactions are lost, the user should re-enter them.

131 In exceptional circumstances, there is the possibility of a transient impact on branch accounts. For instance, in the original Horizon, if there was a network failure followed by a PC failure, there was a slight risk that transactions in the intervening period could have been lost. Similarly, there were issues in single counter branches if the PC failed and was replaced before it had replicated to the Correspondence Server.

132 The impact of such cases should only have been temporary because the principles of double entry accounting, transactional integrity and accounting checks built into the system (and described above) would have detected and thereby prevented any long-term discrepancies.

Appendix R Data Centre Hardware

133 The counter systems used in branches are supported by data centres known as campuses. Each campus contains many substantial hardware platforms. In the interests of simplicity, these use the minimum number of different equipment and operating system types.

134 In Horizon, the platforms supported servers and gateways, PO corporate systems, and management and help desk systems. HNG upgraded the servers and storage devices, introducing newer technologies.

135 For resilience, both generations of Horizon have relied upon two physically secure campuses (the robustness measure RHW). Originally these were located at Wigan and Bootle, with each providing fallback for the other. The campuses had a similar network configuration and servers. Each, and all the equipment in it, was sized to be capable of running the entire workload. The simplified diagram below illustrates the replication and redundancy of major components that help to avoid SPOFs:

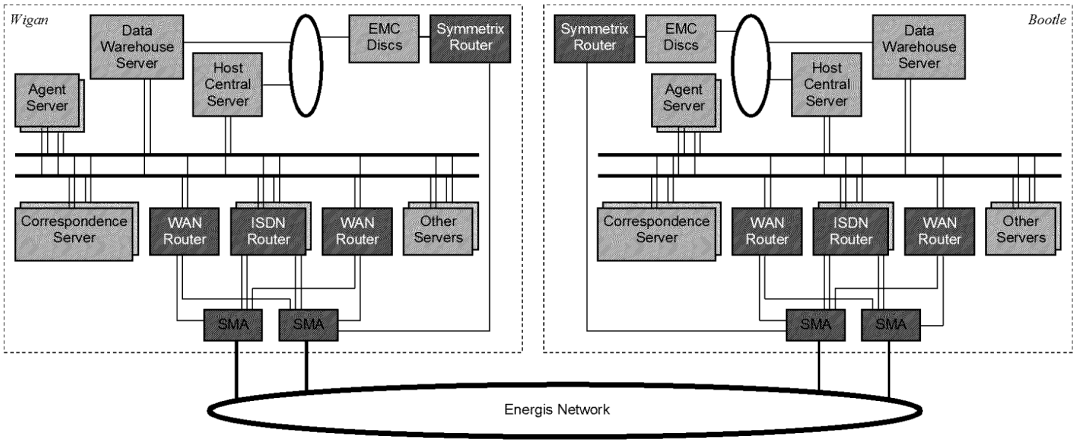

Figure 8.1 – Redundancy of major Horizon system components across campuses

136 Disk mirroring is a technique used to protect a computer system from loss of data due to disk failures. It is a form of backup in which anything that is written to a disk array (on a single site) is simultaneously written to a

3 Description based on https://www.techopedia.com/definition/25959/disk-mirroring

FUJ00082226

second disk. If one hard drive fails, the data can be retrieved from the other mirrored hard drives.[3] This is another example of RHW robustness.

137

138 The resilience strategy for the Host Central Servers (shown in Figure 8.) involves replicating data between the two sites. Thus, following a site failure, the servers at the other site can quickly take over the entire workload. A single disk array is used in each campus. Each array supports internal disk mirroring, with automated recovery from the mirror in the event of a single disk failure.

139 In HNG, both data centres have been relocated to Belfast. One campus supports the live operation while the other provides disaster recovery (DR). Under usual operation, the DR Data Centre is used for testing. Some 'Live' elements of the solution are operational at the DR Data Centre where this is required to support DR.

140 Each data centre can support the entire branch business and is configured so that no single failure leads to loss of service. Data is replicated from the Live Data Centre to the DR Data Centre to ensure that, in the event of disaster, there is:

- No loss of transactions received from the Branch estate where those transactions have been committed to the Branch database.
- No loss of the audit trail

141 Switchover from the Live Data Centre to the DR Data Centre is manually initiated.

Appendix S Branch Software

142 Fujitsu has selected mainstream infrastructure products such as Windows, Unix and Oracle[4]. These products lead the market, because they have proven to be robust and reliable. As far as practicable they tolerate faults, thereby providing a degree of resilience to the solution.

143 The software running within each branch is now quite different to what was included in the first Horizon system prior to the year 2010.

144 In original Horizon, the key software was Riposte. This provided the user interface and messaging infrastructure.

145 Counter clerks rely mainly on EPOSS, which allows them to record that some goods have been provided to a customer, calculate prices and accept payments.

146 As explained more fully in section C.1 , resilience of the branch PC is supported via replication (and automatic recovery) of transaction data across nodes in the network.

147 One of the Horizon architecture documents includes the following principle: 'Applications should be designed and built defensively, so that they can handle any type of unexpected conditions in a controlled manner' [5]. In other words, Horizon software has been built to detect errors and respond appropriately – rather than fail. This is defensive programming (DEP). Any exceptions in lower level components are trapped and handled within the

4 Unix and Oracle are used on servers at the data centres, rather than in branches.

5 Technical Environment Description for the original Horizon system (TD/ARC/001), section 11.6.3.3

FUJ00082226

calling software. Errors are logged, with event notifications directed to support staff so that they can analyse the problems encountered. This is resilience through redundant storage of data (RDS). In our experience, there is a limit to the application of this worthy principle. As error handling is an overhead that can adversely affect performance as well as development costs, it should be included in software judiciously.

Appendix T Data Centre Software

148 As we have explained earlier in this report, Oracle databases and the associated tools have been widely used across Horizon. They provide a resilient platform for the most important applications. Riposte components running on servers also formed part of the picture for tolerating and recovering from failures.

149 In 2001, Oracle introduced Real Application Cluster (RAC). A cluster is a set of connected nodes (computers used as servers) that work together so closely together that they can be viewed as a single system. RAC allows cluster of computers to run the DBMS software simultaneously while accessing a single database. By 2006, in the original Horizon system, RAC had been used to provide resilience in the Network Banking Service but the software is more central to HNG.

150 The most crucial component of HNG is the Branch Database (BRDB). Without it, branches cannot trade. Therefore, its design must support non-stop trading during core hours.

151 BRDB is built on RAC with a four-node cluster, which provides high availability. Each node has four processors, which also provides high performance. The database has no single point of failure. Multiple nodes also reduce the probability that a set of simultaneous failures can cause a complete loss of service. If one node fails, the remaining ones carry on running and the database remains available for use. A standby database is maintained automatically; this allows very fast recovery if a fault takes the live database offline. A disaster recovery site remotely mirrors the data. The mirroring of data is synchronous. This guarantees that no data is lost if there is a catastrophic site failure. All these are examples of the robustness measure RHW.

152 The connection from the counters to the Branch Database is through the Branch Access Layer (BAL) as shown in the diagram below:

FUJ00082226

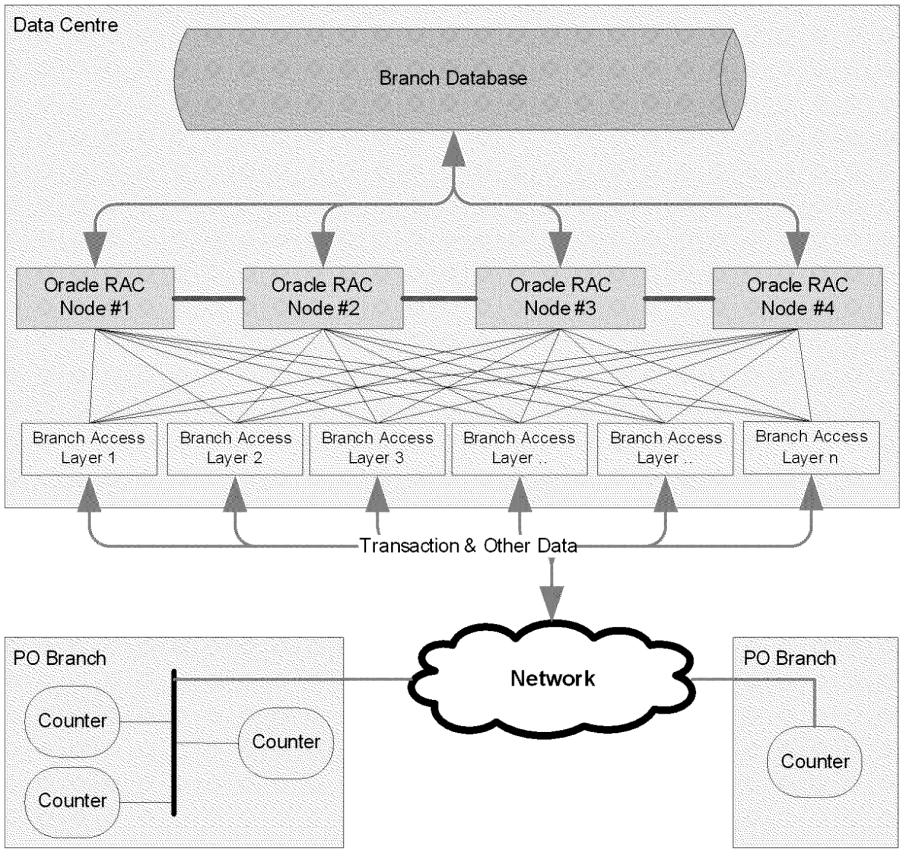

Figure 8.2 - Oracle RAC in the tiered architecture

153 The resilience of application software is underpinned by isolating components across the tiered architecture (as described in section **Error! Reference source not found.**), by the resilience of the platforms supporting them and by the discipline of defensive programming. These are all aspects of the robustness measures RHW, ARC, and DEP.

Appendix U Networks

154

155 Computer networks are built using a combination of hardware and software elements. Examples include gateways, routers, firewalls and virtual private networks (VPNs).

156 The following diagram provides an overall view of the Horizon networks:

FUJ00082226

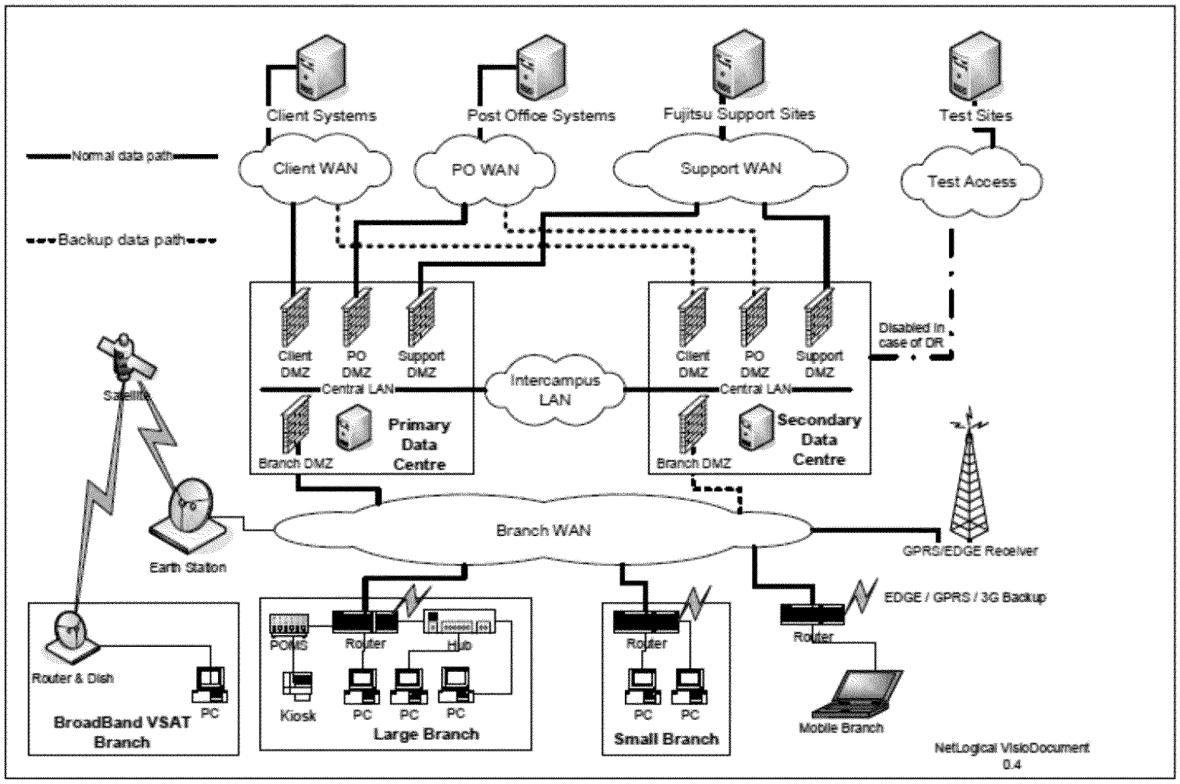

Figure 8.3 - Horizon network overview

157 In the original Horizon, the WAN was built on ISDN[6] connections, although a VPN service was also used between the branches and campuses. Branches could continue to trade with no WAN partly because the connections at that time were less reliable. This feature of the architecture reduced the need for resilience across the Horizon system.

158 By 2006 many of the ISDN connections had been upgraded to ADSL[7]. Branches located too far from an exchange use VSAT[8] satellite technology and mobile branches used EDGE[9], GPRS[10] or 3G[11]. EDGE/GPRS/3G is also used as a backup for ADSL.

159 The communications infrastructure carries networking services over several types of connection with different bandwidth, depending on the needs of the services using that link. Resilience is improved by replication of most networking components with alternative routes being provided, where appropriate, in case a primary route fails. These are the robustness measures RHW and ROC. The branches have network connections that can use either

6 The standards for Integrated Services Digital Networks were first defined in 1988.

7 Asymmetric Digital Subscriber Line

8 Very Small Aperture Terminal

9 Enhanced Data rates for GSM Evolution: GSM stands for Global System for Mobile telecommunications

10 General Packet Radio Service

11 Third generation of wireless mobile telecommunications technology

FUJ00082226

data centre. Either both data centres are connected (using more sophisticated connections) or one data centre is connected normally with the branch able to use the other data centre if there is a problem. The VPN software in the counter connects to multiple VPN servers at both sites to provide resilient encrypted tunnels.

160 The PCs in each branch are connected with each other and to peripherals using a Local Area Network (LAN). One of the local PCs is designated as the gateway through which the branch systems communicate with the rest of Horizon.

161 A Wide Area Network (WAN) connects branches with the two campuses and the Horizon data centres with PO's clients.

162 The key services that must be supported by these networks include the following:

- Transfer of files to and from remote systems; and
- Access to business applications and information running on remote servers.

163 Messages from branches are transmitted to both campuses and their Correspondence Servers. Messages from Correspondence Servers to branches are directed to the IP address of the Gateway PC in the branch, which is known to each Correspondence Server.

164 The ISDN card in the Gateway PC enables it to behave as a normal LAN connection. ISDN call set-up is done automatically when the Gateway PC sends a message over the link. Similarly, a call is set up (if none exists) when a Correspondence Server sends a message to a branch. To avoid too frequent calls, Riposte only sets up a call when an urgent message must be passed in either direction, or when a normal message has to be passed and a "handshake" timer expires. The timer starts at the completion of the transfer of the previous set of messages. If there are no messages to pass, no call is made, so a small branch may not catch up until the end of day. Once a call has been established then all waiting messages are transferred in both directions. The call is cleared down on expiry of an idle timer with a default setting of twenty seconds. An implication of this process is that all communications traffic between the branches and the campus must go via Riposte. There is thus usually some delay between a message being created at a counter position and that message reaching the campus.

165 With HNG, network connections are more reliable. Nevertheless, network resilience remains vital to system availability.

166 A LAN subnet is used between the two campuses. The principal need for this is where a single IP12 address is used by client applications to access a service that runs on a server at one campus but may fail over to the other. For the single IP address to be able to follow the service, the two servers must be on the same subnet. This is implemented by bridging the two campuses to create Virtual LANs (VLANs) spanning the two campuses.

Failure of Communication Link – original Horizon (ROC)

167 When a branch lost its communication link or the Gateway PC, business could still be conducted. Nevertheless, counters could not communicate with the Correspondence Servers, and vice versa. Riposte message replication

12 Internet Protocol

FUJ00082226

would not operate. The branch became progressively more out-of-date, and the campuses had no record of transactions that had taken place in that branch.

168 Certain operations that would normally make a real-time connection to the campus would time out and the user would put in a call to the help desk. When the link or the PC was repaired, Riposte message replication brought the branch and the Correspondence Servers back into line.

169 At first, this was not a significant issue. The software running in branches was designed to detect failures and re-try communications until some limit was reached. The clerk may have needed to take actions, guided by the system.

170 Starting in around 2005, an increasing number of applications relied on being able to contact the campus. Banking and debit card handling were the first two such applications, but more followed. In response to this requirement, two improvements were made to the branch-campus network.

- A Counter Network Information Monitor (CNIM) was introduced. This monitored the status of the link, and if it was not available it informed the user. Once the link was re-established, this indication was removed.
- A new data network was introduced, which enabled more heavily used branches to be permanently connected to the campus.

Network Failure - HNG (ROC)

171 All HNG branches detect WAN connection failures, and switch to an alternative connection type without the need for users to restart their application sessions.

172 A network failure on the LAN is much less likely because of the relative simplicity of the network. If the LAN fails, business transactions for all affected users will be prevented, so users will report the problem to the help desk who will deploy an engineer to repair or replace the faulty hardware.

173 The counter business application is aware of the state of the network by interacting with the CNIM and will not offer services to the clerk when no WAN connection is available.

Appendix V Business Continuity and Disaster Recovery

174 Wikipedia defines and distinguishes these terms as follows: '*Disaster recovery involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity.*'

175 Clearly the biggest risk to continuity of Post Office's business is a disaster affecting the Horizon data centres, but the loss of a complete branch has also been considered.

176 A branch could be lost, for example as a result of fire, flood or the theft of counter systems. In the original Horizon system, there would have been two key implications:

FUJ00082226

- The payment of benefits to customers could have been delayed. However, contingency arrangements were built into the applications that would enable benefits to be paid at any other branch. These were known as Foreign Encashments.
- Any transactions that took place within the branch, but were not replicated to the campus, would have been lost. Where the equipment, rather than the branch as a whole, was destroyed then any outstanding transactions could have been reconstituted from the paper records. Each of the printouts includes the transaction number. When the equipment was replaced, Riposte enabled the system to identify the last transaction number secured at each counter. The remainder could have been manually re-keyed.

177 HNG applications include a wider range of contingency arrangements, commensurate with the additional services provided before any disaster occurred. Because the BRDB is held centrally, the loss of a branch or counter is less problematic than in the original system. Any business being transacted at the time of the disaster is likely to be lost, but all of the previous work will have been secured.

178 DR for the data centres is discussed in sections 6.5.2 and C.4 above.

179 Disaster Recovery depends on a range of robustness measures, including RHW, ROC, TIN, and RDS.

FUJ00082226

Appendix W SECURITY AND USER AUTHENTICATION

180 This appendix provides additional information to supplement section 6.6 of the report.

Appendix X Authentication

181 Authentication seeks to verify the identity of a person (or system component) seeking to gain access to a system resource. Authority may be established using a set of credentials, most commonly a username (or ID) in combination with a password.

182 User authentication is required at specific points within the system architecture. The following types of users are identified:

a) Subpostmasters and counter clerks in branches;

b) Counter PCs that must authenticate when establishing a link to the data centres;

c) PO operations and support users;

d) PO managers, who need to access Horizon and its associated corporate systems.

183 Counter PCs are encrypted to prevent unauthorised access, particularly if they are stolen. See section D.4 below for further details on encryption.

184 In the original Horizon system, the subpostmaster gained access using the Post Office Log On (POLO) process, with authentication provided by the Microsoft operating system (Windows NT at the time). This required the subpostmaster to insert their memory card into the PC keyboard and enter a PIN. The authentication process validated the PIN against information stored on the card. If that was successful, the POLO process used information from the card to decrypt the PC.

185 Login was controlled by the Riposte software, supplanting the basic Windows NT system to improve login and logout times.

186 The counter clerk submitted their user ID and password via this screen. Riposte used standard Windows NT to authenticate users, passing on the passwords to be hashed and compared with the value stored by Windows NT.

187 PCs operating in branches need to authenticate themselves when they connect to the campuses. Section C.5 above summarised Horizon's networking technologies. In the original system, the gateway PC[13] in each branch periodically established a link with a campus during which all outstanding messages in either direction were exchanged. ISDN-connected branches originally used Microsoft's proprietary Remote Access Service (RAS) to authenticate themselves. However, this method was superseded by a mechanism known as VPN, which provides an encrypted channel (or tunnel) between the counter PC and the campus. Sessions are established using a VPN key distributed by a central server. The ability to initiate and respond to an encrypted connection using this key proves the identity of the branch.

188 The processes described above are used for counter PCs only. Where users needed to access the Windows NT servers or workstations located in the campuses or support centres, conventional Windows NT authentication methods were used. Similarly, servers such as those running Sun Solaris supported standard login authentication

13 One of the PCs in each branch was designated as the gateway through which communications flowed with the rest of Horizon.

FUJ00082226

provided by Unix[14].

189 Horizon's access control policies stated that people accessing Horizon systems had to identify themselves using hand held tokens if:

- they were at sites remote from the Campuses and could update the operational systems (for example, for management purposes);
- they had access to PO business data (except at branches);
- they were authorised to update system data (such as reference data), which can affect the running of the main operational systems. This included anyone with system and database administration privileges.

190 Horizon used SecurID tokens (from Security Dynamics) as tokens. All accesses authorised in this way were audited.

191 Oracle DBMS authenticated either via the underlying operating system or directly by the Oracle database itself. Direct login to the Oracle database applications was restricted to Oracle support. Each of these had a unique user ID and password for the database (as well as separate Windows NT credentials).

Appendix Y Roles and access control

192

193 Access control is achieved by verifying that a particular user is only able to access a given resource in an approved manner. It is defined in terms of roles, each of which defines a number of functions that a user can perform. A user may be allowed to assume several separate roles.

194 Roles were initially defined as follows:

- Post Office - including manager, counter clerks and auditors;
- Operations - provide the means to control the Horizon systems during normal running;
- System and Security Management - provide the means to maintain and monitor the system, including adding new software and users;
- Support Roles - such as engineers and applications support.

195 Control of access by other computer systems is as important as control of access by people.

196 Firewalls make an important contribution to access control by protecting one part of a computer network from another. They only allow traffic to flow between a defined set of network end points on either side of the firewall using specific services. Firewalls also perform other functions such as:

a) Preventing certain users or machines from accessing certain servers;

e) Monitoring communication between networks;

f) Eavesdropping;

g) Controlling what can be sent across the firewall.

14 Unix is the most widely used operating system not owned by Microsoft.

FUJ00082226

Appendix Z Virus infection

197 The threat of virus infection in the original Horizon system was relatively low:

- Although the counter PCs were equipped with diskette drives, these were disabled except where they were required for transfer of encryption keys.
- There were no e-mail connections to external systems.
- Microsoft Word documents (which could contain Word macro virus) were rarely imported.
- Operational files transmitted by file transfer contain only data (rather than executable code)
- The main processing platforms were Unix based, which was less vulnerable to attack.

198 There was, nevertheless, a need to protect against the introduction of viruses from the following external sources:

- Executable files introduced for maintenance purposes;
- Microsoft Office documents;
- HTML documents containing user Help information.

199 All workstations other than those in branches had virus protection software installed, which was updated regularly as new definitions and software versions were received.

200 All executable code was virus checked prior to being imported into any part of the system.

201 All Microsoft Office (and HTML) files were vetted for macro viruses before they were imported into any part of the system.

Appendix AA Encryption

202 Encryption is the process of encoding a message or information in such a way that only authorised parties can access it. Information is encrypted using a key generated by a special algorithm. An authorised recipient decrypts the message with the key provided by the party who sent the message.[15]

203 Horizon used encryption for three main purposes:

- to protect data on communications links that pass outside the control of Horizon, its suppliers or customers;
- to protect the integrity of individual messages from creation to use;
- to protect the confidentiality of data stored on physically insecure systems such as counter PCs.

204 A widely used encryption scheme is known as public key infrastructure. PKI uses asymmetric cryptography with pairs of keys: public keys which are shared widely, and private keys which are known only to their owners. This accomplishes two functions:

- authentication, where the public key verifies that a holder of the paired private key sent the message, and;

15 This description is based on the following reference https://en.wikipedia.org/wiki/Encryption.

FUJ00082226

- encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

205 In a public key encryption system, anyone can encrypt a message using the receiver's public key. That encrypted message can only be decrypted with the receiver's private key.

206 The original Horizon system used five types of encryption:

a) Symmetric encryption - for files stored on counter PCs

h) Asymmetric encryption - to seal messages for integrity, but it was not used to encrypt data

i) Digital signatures - a digital signature is a code (generated and authenticated by public key encryption as described above) which is attached to an electronically transmitted document to verify its contents and the sender's identity. A valid digital signature gives a recipient confidence that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

j) One-way encryption – where the results could never be decrypted, e.g. for passwords. The original value is one-way encrypted, and the result is held within the computer system. If a user supplies a value that yields the same encrypted value, then it can be assumed that the data supplied was the same as the original data. Another use for one-way encryption was to generate a seal for a piece of data. A hash value is generated which is dependent on the entire content of the data to be protected. If the hash value is re-generated later, and found to be different to the original seal, then it can be assumed that the data has been tampered with.

k) VPNs - all traffic flowing between branches and campuses was encrypted using a variant of asymmetric encryption.

207 Horizon key management was based on the ISO 11770 model.

Appendix BB HNG

208 Many important principles of security were established in the original Horizon system, as described above. While HNG honours many of those, the architecture has been rationalised in that the choices are based on an updated assessment of the risks faced by the system. The security architecture has been developed with the aim of ensuring that there are no single points of failure and that each area of risk has more than one technical or management control working together to mitigate that risk.

209 The solution has been architected using the control objectives in ISO 27001[16] as a guideline.

Encryption

210 HNG still makes extensive use of cryptography and digital signatures for the protection of data, both in storage and during transit. AES[17] or TDES

16 ISO 27001 provided requirements for an information security management system - a systematic approach to managing sensitive information so that it remains secure. It includes people, processes and IT systems and applies risk management techniques.

17 The Advanced Encryption Standard is a specification for the encryption of electronic data established by the U.S. National Institute of Standards

FUJ00082226

211 [18] encryption keys and RSA[19] signing/encryption keys are now used. Messages from the counter to the data centre are protected by a combination of VPN technology and SSL[20]. These transaction messages are also digitally signed.

212 Connections to third parties are protected through the use of encryption where the contractual agreement requires that.

Identity and Access Management (User Authentication)

213 The authentication of users is performed by a directory service. This includes Unix operating systems as well as Microsoft Windows. This is achieved using Active Directory as a master directory service with the implementation of a separate authentication module on non-Microsoft platforms. This enables the non-Microsoft platforms to appear as objects in Active Directory and facilitates central access management.

214 All users of the Horizon system are individually identified, through a process controlled by the Security Team. Every administrative user uses strong two-factor authentication when logging on to the system and it is not possible to directly access any Horizon system without such a token.

Payments

215 HNG meets the requirements of the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI DSS is an information security standard for organisations that handle credit cards. It was created to increase controls around cardholder data to reduce credit card fraud, and it now provides a comprehensive framework of good practice.

---

and Technology in 2001.

18 TDES is an abbreviation of Triple DES (or Triple Data Encryption Algorithm), which is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

19 RSA forms part of a PKI, providing asymmetric encryption.

20 Secure Sockets Layer encrypts data sent via the Internet.

FUJ00082226

Appendix CC ANALYSIS OF KELS

Appendix DD Purpose of this appendix

216 This appendix contains some tables of KELs which are referred to in the report. The tables are:

a) A sample of 30 randomly selected KELs (selection of every 100th KEL in an alphabetically sorted list), with commentary on the robustness countermeasures which acted in the case of each KEL, as well as its potential financial impact.

b) 62 KELs mentioned in Mr Coyne's report, for which I have also analysed which robustness countermeasures applied and analysed the possible impact on branch accounts.

c) Eight KELs which were mentioned in the claimants' outline of 17th August, which I have had time to analyse in more detail than other KELs mentioned in Mr Coyne's report - but without analysis of countermeasures.

d) A further sample of 50 randomly selected KELs (also every 100th KEL in an alphabetically sorted list) which I have analysed for possible financial impact, but I have not analysed for robustness countermeasures.

217 There is some overlap of KELs between the different tables, because of limitations of time in preparing this report. I intend to present a fuller analysis in my supplemental report.

Appendix EE My 30 KELs with countermeasures

218 In this table, for some KELs we can say there is no financial impact on branch accounts. In those cases, the entry under 'financial impact' is 'No'. In cases where financial impact is possible or likely, the entry is 'yes' and we have quantified it, as in the next section. This usually results in a very approximate estimate; but where the estimate is very small.

219 For some of the KELs. it is not possible to say definitely that there is no impact on branch accounts, but we have found no evidence in the KEL or related Peaks that there is any impact. In those cases the entry under 'financial impact' is 'no evidence', and we have not attempted to quantify any financial impact.

FUJ00082226

and title, and Peaks	Date Range	Extracts from KEL or Peaks	Analysis	Robustness summary	Financial Impact?
3L nce pouch barcode not recognised at newly-opened branch 086	8/11 - 10/13	Replenishment delivery information is sent to branches in files from SAPADS. If the branch is not Open in RDDS at the point the file is processed by LFS, the pouch contents will not be put into the Replenishment Delivery table on BRDB and so the pouch contents cannot be auto-remmed in. The branch should rem in the cash etc manually - NBSC can advise them on the process. Note that they are prompted to enter two values, the total pouch value and then the same amount again as confirmation.	In this case, an automatic process (the remming in of cash) was failing in a manner evident to the branch, and so the branch had to do the process manually. The KEL contained advice to help them do this. The error only occurred in rare cases (newly opened branches) over a short period of time. If the branch remmed in cash manually, then no error was introduced. Even if the branch failed to do this, the error would be evident in the monthly branch balancing process and would be corrected then.	Manual workarounds applied (WOR). If these were not done correctly, UEC would later correct. Double entry of the pouch value is DUE. An error file was created, possibly by ROC/DEP.	No
S ORD RT100000 reports produced by APOPX016 017	3/12 - 11/12	Three postal order reports should be produced on Sunday nights, every 4 or 5 weeks when the date matches the APOP_ACCOUNTING_PERIODS end, by APOPX016 / schedule APOP_PO_REPORTS. Reports not produced end March 2012 because accounting period end date was Monday not Sunday (PCPC0216908). Ref data check implemented to try to prevent this in future.	The KEL refers to the APOP host, so it is about a report produced at the centre. The lack of any such reports has no impact on branch accounts.	In this case, a reference data check was implemented (BFC).	No

FUJ00082226

ɔers525P hangs during EMV transaction 77	5/05	[there is a complex analysis of why a counter may hang. in certain conditions] If a PM phones in about this problem, they should be advised to reboot, and to log back in to the counter as soon as possible so that any incomplete transaction is automatically recovered. If this is happening frequently at any one site, send call to SSC.	The counter could also hang for any hardware fault, and normal recovery is designed to handle this without any impact on branch accounts.	Normal recovery of a counter depends on TIN, RDS, ARC. WOR was applied. BFC - a fix was scheduled in release S90.	No
allend230Q ception - Serious system error: Unexpected Message Body ... 404 Not Found 034	9/10 - 8/11	Call to a web service fails, with an OSR log entry of the form: ERROR ... Serious system error: [Unexpected Message Body<!DOCTYPE..... The error is part of the remote WEB Service response. The OSR handles it in this way because this is unexpected behaviour and shouldn't happen. It is an exception case which by design would result in a timed out response on the Counter.	OSR = Online Service Router – the component in the Branch Access Layer that connects the Counters to Agents Web services are typically used to call an external client. They are expected to time out on some occasions, with no effect on branch accounts - because system design must not allow for them to time out. Getting a different error message instead of a timeout message should make no difference.	Standard architecture for web services has to be robust against communication failures and timeouts, which happen all the time (ROC, ARC, DEP)	No

FUJ00082226

ArnoldA1229L T FOR UPDATE missing 425	10/09	While inspecting the code we have observed that there could be problems with race conditions such that one user's change could overwrite another user's change without warning. There are a number of cases where SELECT statements should be SELECT for UPDATE to ensure that multiple counters in a Branch can't interfere with each other before the row is Updated. The SQL statements affected are: • SelectPSBarcodeCollectionStateInSettlement • SettlePouchDeliveryPreCheck • SUTransferOutPendingStateQuery This is very unlikely to happen so can be deferred.	The date of the Peak (September 2009) and the target release (HNG-X CTR022) imply that this was a fault found in testing, not in live use. Because the error condition was 'very unlikely to happen' it was given a low priority (D) and is not expected to affect branch accounts.	Finding the error in testing, and assessing its importance appropriately, is TGP.	No
ArnoldA4855N TES data availability - 2nd supporting request PC0177950	10/09	In order to extract data from the DWH and present it to the DXC for reporting purposes on TES Data Availability during a TES failure condition we need to add "TOTAL_MSG_OVER_ABS_LIMIT" to the TES Data Availability extract from the DWH Host system. This is a low priority change which should be done when resources are available.	TES = Transaction Enquiry Service. This is a central reporting issues, with no impact on branch accounts.	To assess BFC, we need to see the Peak. It appears to be nothing more than a low priority change.	No

FUJ00082226

AshokP134G BRDB PROPAGATION PROCESS: ABORTED No Peak.	11/09	Raise a B priority TFS call and send it to the HNG DBA Support TFS Stack for investigation.	This is a brief and cryptic KEL, with no associated Peaks. 'propagation' refers to transferring data from some other system or systems to BRDB. One such system was OCMS; if that propagation was being referred to, the data had no connection with branch accounts. In any case, if a propagation process was aborted, this would stop transferring data, rather than transfer erroneous data. There would need to be a recovery process to ensure that all data was transferred correctly, so there is no possible impact on branch accounts.	Little evidence. Robustness of transferring data between databases involves TIN, which BRDB has.	No
bakert2250I Template Structure wrt caching (raised internally by Dev - Peak 173116)	11/09	A problem was identified where a reprint of a receipt was not re-printing the correct duplicate of the original because it was picking up data from outside the printable object (e.g. $System or date functions).	This bug was found in testing and was corrected. The conditions for it to arise meant that a user would have to change stock unit and then ask for a reprint – not a likely scenario. In any case, incorrect printing of a receipt is unlikely to lead to the user subsequently making a mistake.	The bug was found in testing, which illustrates TGP.	No
bakert58K move viewport stuff to UI PLAF PC0172530	10/09	Replaces Bugzilla 1676 Call Type changed to Enhancement Request(E) Moved to Deferral stack, but need to be individually checked at some point	The Peak shows that t this was a bug detected in testing. It was subsequently changed to an enhancement request. This indicates that it was not regarded as a bug which could impact the branch in any material way.	The bug was found in testing, which illustrates TGP.	No

FUJ00082226

BFoster286K The specified persistent object was not found, RemoveObjectEx: Runtime error 450 PC54767	10/00 - 12/00	Counters Windows NT event log displays the following "The specified persistent object was not found. (0xC102001D).... "A problem has been found is CASEPOSSEVProducts.exe whereby the routine which tidies and removes ProductChanges entries older than 90 days will always fail with a VB error whenever it finds something to remove... A fix for this problem has been produced under PC0054279 for CI4R and is going through testing. This problem is more of an annoyance and should not affect the operation of the counter. Fix released in WP9951 CI4M1	As this was 'more of an annoyance and should not affect the counter' there can be no impact on branch accounts	The bug was detected as a runtime error, as a result of defensive programming - DEP The event log illustrates RDS, MID	No
BSheldon3110K SPSupport warning events PC122737	7/05	When counters are migrated to S80, with the S80 ref data loaded. Two warning events are raised relating to SPSupport every time the Desktop is loaded. These events can be safely ignored, as there should be no issues with SPSupport not being able to find this data ahead of the S80R data delivery, as the S80R delivery will presumably be the first time the T&T menu buttons are delivered.	Warning events should have no effect on branch accounts.	Warning events are DEP, MID.	No

FUJ00082226

cardc3335R Vodafone Text Pack Vouchers being declined PC0184509	7/09	Vodafone £10, £15 and £20 Text Pack Vouchers are being declined. However Vodafone £5 Text Pack Vouchers are being authorised successfully. The reason for the Vodafone £10, £15 and £20 Text Pack vouchers being declined by epay is because they were deactivated on request by Vodafone.	System correctly refused to do a certain kind of transaction. There can be no effect on branch accounts	The extent of the problem was rapidly identified by inspecting the DRS database (MID) The problem was easily fixed by updating reference data (BFC, DDS)	No
ChahalS1943S Bootle_NPS_Cluster on SBONPS01 Based on: SBONPS01.VCS alert (SAMBA) No Peak	12/06 - 1/07	Samba is a unix program that allows filesystems exported from Unix hosts to be mounted on Windows systems. Within the NPS cluster configuration samba is used to export the audit and Metron directories to the appropriate windows platforms.	This is a back end batch problem, not affecting any specific branch. Solutions were proposed, which presumably let the back end processing proceed. In the absence of any further evidence (no Peak) we can assume it did not affect branch accounts.	The problem was rapidly revealed by service monitoring tools and alerts (DEP, MID) Operational solutions were defined (BFC)	No
CharltonJ4634R Unable to roll over - Reference Data Error message PC0198818	5/10 - 11/15	The accounting period reference data for the named year is missing from the counter. This is most likely to be because the data has been end-dated and removed from the working day set. This may occur when the PMs fail to rollover the counters in a timely manner. To correct the Branches which are running in an old/expired Financial Year, the SSC Team will need to perform a chargeable activity	These branches needed assistance to roll over. There is no evidence that it caused problems in their accounts.	When it occurred (though user error) the problem was immediately obvious (UEC, DEP) Fixes to the problem were identified, which only involved changing reference data (BFC, DDS)	No evidence of impact

FUJ00082226

ClaudV3457L OEM 12c Oracle Management Server is not reported as up No Peak	3/16 - 2/18	the alert about OEM 12c Oracle Management Server is not reported as up - this is the web interface for users to logon to OEM	The mention of Oracle implies this is a back end problem. While there might be a causal chain to affecting branch accounts, it would be obscure and there is no evidence for it here. It was an operational problem about starting an application, not a software error	This was an operational problem, revealed by monitoring tools (DEP, MID) Operational solutions were defined (BFC)	No evidence of impact
CroshawM323S CS -H21584300101-LockdownMgr-Function: ReadRegistry returned Win32 Error PC0195344	3/10- 12/10	ReadRegistry returned Win32 Error: 2 Description: The system cannot find the file specified. Appears to be a registry error, but not known exactly what causes it. Only occurred once on the counter specified in the PEAK.	Analysis by the support team concluded that the event is harmless and can be ignored	The problem was identified by system monitoring tools (DEP) FJ failed to identify the cause of the error (failure of BFC?). It was sufficiently low priority, with no business impact and infrequent occurrence , as to need no further investigation.	No
DDutton3615R The PSEXESVC service failed to start due to the following error: The system cannot find the file specified TFS 510180747	10/05	A Critical NT event was seen at 16:14:44 on 18/10/05, Hostname: MBOCOR01, Source: Service_Control_Manager.	The hostname MBOCOR01 refers to a back end machine, not in a branch. Failure to start a back end machine would not affect any branch accounts..	Critical event seen by MID Unexplained event, no Peak, Failed BFC? Further investigation was done - we do not know the result.	No

FUJ00082226

DGriffiths3514T arms_ACDB: data extract from omdb returned an error TFS 412041211	12/04	Very little detail and no PEAK.	OMDB = Operational Management Database. OMDB is a back-end system. Operational management issues come up frequently, and should not affect branch accounts. There is no evidence that this one did.	Error detected by MID; little else in the KEL	No
DNewbury1848N IP address prohibited to local security policy TFS 309120456	09/03	NWB Eacrr Server monitors bad alert on MWIVPN12 @09:16Communication to ip address 3.2.24.1 prohibited by local security policy. NSID type UNKNOWN is not supported	NWB is the DRS specific abbreviation for Network Banking. The alert came from a back end server , saying it could not connect to an IP address. This is a back end issue which would not impact on branch accounts	This is another one-day KEL with no outcome, like the last two. Illustrates MID.	No
DSale346S Data Ferret queue showing ERROR for Satellite sites. PC105471	11/05	When a Satellite outlets is rolled out after S60 the Data Ferret for the Boot Server DELIVER tasks fails with 'Value for ISDN_PSTN_TEL_NO not available. The ISDN_PSTN_TELNO which used to be the name of the boot server file has been replaced by the H number. The ISDN_PSTN_TELNO is no longer required as an argument and as such any Data Ferret for the Boot Server DELIVER that is in ERROR should be set to COMPLETE	A data ferret is A SYSMAN process used to populate internal tables with data from external sources. Typically used to ensure that data (x), that may arrive after a scheduled process 'P(x)' has been queued, would be available before 'P(x)' is executed (from document 138142123) This is a problem setting up a connection to a new satellite branch.. So if not fixed, it might stop the branch being set up - but that would not affect branch accounts.	Another one-day KEL, a problem detected by MID. Whatever the outcome , we are hardly likely to see it from the KEL. ATOS provided a solution. (WOR)	No

FUJ00082226

dsed4621K The balance report shows negative values for one or more foreign currencies	5/07	In this case the office had done some txns involving Thailand Baht and New Turkey Lira during the balance period. The office had zero holdings of these currencies when it came to doing the trial balance. For some reason, the automatic currency revaluations that should have taken place when the trial balance was produced didn't happen. There should have been a 0.83 revalue up for Thailand Baht and a 1.88 revalue up for New Turkey Lira. Could see nothing in the event or audit logs to explain why these revaluations did not occur. The PM didn't notice anything was odd and carried on with the final balance. It wasn't until the next trial balance was produced that the auto revaluations occurred and the negative values were cleared from the report. It sorted itself out in other words. Forward call on to the SSC if this is seen again as we may need to investigate further to find out why the revaluations didn't happen.	This was a transient problem - which in any case was only a fault in a printed report. If that had induced the PM to make a mistake which affected branch accounts, a later TP balance would have revealed it, by hand count of foreign currency. So there was no permanent effect on branch accounts.	A one-day KEL. Trial balance is UEC. Audit logs are RDS, MID 'It sorted itself out' is UEC Rare circumstance. No Peak or TFS for use to investigate further. May not have been investigated further by SSC if it did not recur	No

FUJ00082226

DSeddon463L Lines missing on counter cash account, possible Receipts and Payments mismatch PC109692	10/04 - 01/05	The cash account lines not matching report (TPSC268A) was reporting differences for an office. For three CA lines the host amounts existed but the counter amounts didn't. The printed cash account produced at the office was missing the same lines and the CashAccLine messages for these lines were missing from the messagestore. No error messages had been written to indicate missing mappings. In one case, the missing lines included the Balance due to PO (line 1085) and PAYMENTS line (1700). This caused a receipts and payments mismatch, reported on TPSC256 The reason for the missing lines was found to be a corrupt GlobalObjects.dat file. From the Peak: Have replaced the corrupt copy of GlobalObjects.dat with a valid copy. We'll see what happens when they produce a cash account this week. The counter produced a 'perfect' cash account this week so replacing the corrupt GloablObjects.dat obviously worked.	This appears to have been a one-off effect in one branch, caused by a corrupt file which was replaced. Therefore no effect on branch accounts.	Triggered by reported differences (RDS, MID) GlobalObjects.dat file was reference data (DDS), rapidly fixed (BFC)	No
G1347 No Entry sign on Memo icon	9/00 - 11/00	This a system feature and the Memo icon will remain unavailable until they receive their first message. Once a message has been received by the counter, the No-Entry sign will disappear. It is believed that no messages will be sent until all counters have been successfully migrated to CI4. This is a feature and not a problem.	No possible effect on branch accounts		No

FUJ00082226

GCSimpson317T Validate and resend an APS file	9/00 - 11/09	An APS client transaction file has failed to be sent due to it failing validation. This is shown by the lingering presence of a file with .LCK extension which will be alerted on by Patrol. From the Peak: Resolution Details: Update by Catherine Obeng: Category 62 -- Final -- No fault in product: Contents of file UU001453 looks 'normal' and so should not have caused the Client any problems in receiving it. There is no fault in any part of our [Fujitsu's] systems. My advise to the customer is for them to contact CSC who handle AP client files before they are sent finally to the prospective Clients.	No fault in Horizon.	Patrol alert is MID. Advice to customer is WOR	No
GMaxwell1859N Track and Trace Barcode Scans & Despatch Report Slow	10/05	PM reports that the Mails T&T Despatch Report takes a long time to run (20 minutes at a 14 counter site). Performance issues have also been reported when scanning a T&T barcode - these taking in excess of 3 minutes to process. Note - this has been reported at Pilot sites 009941 & 062941	This was a performance issue found in some branches when a new facility was introduced. No impact on branch accounts		No
GMaxwell574P An expected build component object was not found (0xC1130011)	7/03-8/03	S40 commit was regressed after rendezvous failures:...	S40 was a new release. This was a problem moving to a new release because of a build failure in the branches. Staying with an old, proven build would not introduce errors in branch accounts	Rendezvous failures are probably RDS	No
GovindarajS3617U Has never been run	9/16 - 8/17	This alert observed from LPRPR3D002, update on TFS A16558757 from Accenture: This error is related to archive log backup in PLE database. This error can be ignored as backup team take backup through RMAN tool not SAP brtool that is the reason backup status is not visible from SAP level.	Archive log backup is back end, and very remote from branch accounts - can have no effect. In any case the error 'can be ignored'.	The alert is MID. The log backup is RDS.	No
hawkesc3050J Branches on dial-on-demand ISDN report slow running, or transaction timeouts needing retries	10/13- 3/14	Only affects branches using ISDN in dial-on-demand mode (NST 24). Can affect any type of transaction on all counters at the branch. May be reported in many ways, such as: slow running, transactions take a long time to complete, transactions time out and need to be repeated, intermittent slow running etc.	This is a type of performance problem (slow running) which does not in itself affect branch accounts. Sometimes it may trigger a fairly normal error recovery situation, as of interrupted communications. No effect on accounts expected.		No

FUJ00082226

HulmeJ2659M Consignment transactions show incorrect unit price on counter release 16.24	8/17	Consignment transactions show incorrect unit price on counter release 16.24 The amount charged to the customer is still correct. A 16.24 hotfix is being considered.	An error in a printed customer receipt does not affect branch accounts.	Detected by MID	No
JAnscomb223N TESX368 taking over an hour to run	2/05	This job runs at 04:00 and checks that TES_COHARV_MON is at a state of succ. The cause was the problem was largely the analysis was too extensive and on too large a sample.	This was back end performance issue. There is no evidence it did anything wrong, other than run slowly	The check is DEP	No

FUJ00082226

Appendix FF Mr Coyne's 62 KELs with countermeasures

CHARTERIS

220 Mr Coyne mentions 62 KELs his report. In this table, I have analysed for each which robustness countermeasures applied and analysed the possible impact on branch accounts.

FUJ00082226

Para	KEL id	Peak or doc Ids	Expert Issue addressed	Analysis	Impact
5.10	wrightm33145J		1- receipts/payments	See my detailed analysis following Gareth Jenkins. DEA in the BRDB did not catch it because the BRDB operation was not double entry.	£20,000 - reimbursed
5.21	acha1233J		1- cash management	Analysed previously (as a pound KEL, containing '£'). Problem affects cash management, not branch accounts	-
5.22	acha1717T	PC0202239	1- cash management	In the Peak: Ann Chambers investigated and found a possible explanation of the £240 from a human error. (MID) The SPM accepted this.	-
5.23	acha621P		1- cash management	Analysed already in report. Errors in cash remming in and out are frequent and obvious in their effects. They are usually corrected by TCs - but if not, will be corrected manually. (UEC)	-
5.24	LKiang3014S		1- cash management	Analysed already in report. Since the problem was obvious to SPMs if the amount was significant, and there was then a simple workaround, it is not expected to have significant effects on branch accounts (WOR) Small effects might not be noticed.	Small
5.24	MScardifield2219S		1- cash management	Analysed previously. the KEL also says that ' These will in turn show up as future inconsistencies (e.g. nothing gets lost in the end).' This refers to the fact that any remaining inconsistency will be corrected in monthly balancing, lending to a correct position. (UEC)	-
5.25	DSeddon5426P		1- cash management	Problem was detected by system events (RDS), would have been detected in POLSAP (DEA) and corrected by a TC (UEC). In any case, the problem was prominent to the SPM, who would ensure it was corrected	-
5.26	acha194L	Stubbs WS	1- cash & kiosks	Analysed previously. The business impact of the error is on cash management and delivering cash - that is, the cash needed at a branch may be incorrectly estimated, leading to late or insufficient cash deliveries. This is not an effect on branch accounts.	-
5.30	DSeddon314Q		1- ref data	Reference data - Queens birthday commemorative coin - an error in reference data caused by a rare circumstance Impact was a remming error, like a manual remming error, which would get fixed by a TC (UEC)	-
5.31	johnbascoG5222H		1- ref data	The KEL says ' Additionally, the reference data is verified and there is no client accounting code with 3046 '. So, there was no fault in the reference data. The fault was impossible to reproduce, and so not understood. Failure to complete a transaction would not produce an error in accounts - a double entry transaction would either all succeed, or all fail (TIN, DEA)	-

FUJ00082226

5.32	acha10L		1- ref data	This was a fault in reference data, corrected the next day. Failure to complete a transaction would not produce an error in accounts - a double entry transaction would either all succeed, or all fail (TIN, DEA)	-
5.33	MWright1458Q		1- ref data	This was caused by a user error - failure to rem out products when they were withdrawn. The reference data was not at fault - it was changed correctly, but later the user was unable to rem out the products. This left the user with a problem she could not solve herself but needed PO support to do so (WOR). The result was no error in the branch accounts.	-
5.34	wbra5353J		1- ref data	Already analysed. This was a fault involving a kiosk, which resulted in a customer being debited three times, after which the session was cancelled. This would be a recoverable transaction because it involves a credit card; cancellation and subsequent recovery would lead to no net effect on the branch or the customer. The fault appears to result from two causes: (a) faulty reference data, which was easily corrected, and (b) a fault in the kiosk software, which came from an external supplier, and was outside PO/Fujitsu control.	-
5.38	GMaxwell3651K		1- duplicate transactions	This poses little threat to branch accounts because: • A back-end error like this, sending duplicate transactions to a client, would probably involve several branches in the same way - an obvious pattern, not the branch's fault • Usually one would expect the client to detect the error by manual inspection - as happened in this case (MID) • If not, it would lead to reconciliation failures with that client. Investigation would show the same pattern for several branches- i.e. not branch error (RDS, MID) • In the last resort, audit data would show what each branch actually did, with no duplicate transactions (RDS, SEK) So, it is handled by some combination of RDS, MID, SEK - as it was in this case.	-
5.38	surs357P		1- duplicate transactions	Same incident as previous KEL - same analysis. KEL also says: As no customer accounts have been debited twice no further reconciliation is needed.	-

FUJ00082226

5.41	jharr832S		1- failed recoveries	This KEL just notes that recoverable transactions are complex, and, because they are relatively unfamiliar to clerks, prone to human error. CHARTERIS Generally, human errors in recoverable transactions (i.e. failure to recover properly) lead later to a TC with the client affected, and to correction in branch accounts of the impact of the failure. (UEC). The KEL refers to an Ann Chambers note which I need to see.	-
5.42	cardc464Q		1- failed recoveries	This KEL does not indicate any software error, just a failure to recover a transaction involving a timeout at the BAL Normally, any failure to recover a transaction results eventually in a TC which corrects any error in the branch (UEC) So there is no impact on branch accounts, as Mr Coyne acknowledges	-
5.43	seng2037L		1- failed recoveries	This is a complex KEL which describes what to do in a number of circumstances in network banking reconciliation. Some of them are described as needing manual recovery, but it is not clear whether or not, without manual recovery, they would later lead to TCs with an opportunity to investigate and correct any error. Needs further analysis.	possible
5.43	acha959T		1- failed recoveries	This is another complex KEL with strong overlap with the previous KEL. Needs further analysis.	
5.44	dsed4733R (no 20)		1- failed recoveries	This KEL refers to a failed recovery report (report of failed recoveries), and some unexpected items in it The existence of the failed recovery report is evidence of routine robustness countermeasures (RDS. MID) to deal with failed recoveries. In this case, the unexpected behaviour seems to have arisen from faulty reference data, which one would expect to be corrected quickly (BFC). In the meantime, manual corrections were made (WOR). So, there is expected to be no impact on branch accounts.	-

FUJ00082226

5.51	PSteed2847N		1- failed reversals	This describes a software fault that resulted in inability to reverse a remming transaction. As with all other remming errors (including human errors), if there results a discrepancy between physical cash and the Horizon record, that discrepancy will be corrected in balancing at the end of the TP, with no adverse effect on branch accounts. (UEC) The discussion in the KEL appears to be about correcting the error before this backstop was needed The software error was fixed in about two months.	-
5.52	cardc5756N		1- failed reversals	This was an error remming in a pouch and trying to reverse it. As the clerk appeared to have followed the correct procedure, it may have been a software error, but it could not be reproduced As with all other remming errors (including human errors), if there results a discrepancy between physical cash and the Horizon record, that discrepancy will be corrected in balancing at the end of the TP, with no adverse effect on branch accounts. (UEC) The discussion in the KEL appears to be about correcting the error by an earlier TC before this backstop was needed	-
5.54	GCSimpson1049L		1- unclassified	Foreign currency doubling up - very brief KEL, under investigation. Need to see the Peak for subsequent history. Generally, human errors in handling foreign currency (leading to discrepancies between the Horizon record and physical cash) are corrected in monthly balancing and rollover (UEC). So, if a software error had this effect, usually one would not expect it to have any permanent effect on branch accounts.	-
5.55	MHarvey3527I	PC113202	1- unclassified	The KEL says: 'As this is, at the moment a one-off event and clearly no further progress can be made at this stage, I have therefore closed PC113202 as "insufficient evidence". However, any further occurrences should be sent to APS Counter Dev for investigation.' Clearly in a highly complex system, there are occasional one-off events, caused by circumstances not fully understood or observed when they happened. At this later stage we cannot understand them nearly as well as the support team could at the time and should not read any significance into them.	

FUJ00082226

5.56	CObeng1123Q		1- unclassified	This was a memory loss issue which appears to have been perplexing at the time. Extensive searches were found for memory loss issues in the release under test at the time, and only one was found and explained. Occasional perplexing issues, such as this one, are to be expected in complex systems. If this was perplexing at the time, to investigators familiar with Horizon, it must be more perplexing to the experts now, and we cannot draw any conclusion from it which will assist the court.	
5.57	DRowe1625K	PC0084116	1- unclassified	KEL not found. Archived?	
5.68	dsed525Q		1- hardware; pin pads	This was a faulty PIN pad. It prevented the SPM from doing some transactions - but this would not corrupt branch accounts. Normal countermeasures against hardware faults would apply - in this case, that either a complete transaction would be recorded, or none at all (TIN)	-
5.68	surs3941P		1- hardware; pin pads	This was an apparent failure of a PIN pad. In this case it appears to have been caused by trying to use a credit card for a balance enquiry - which it cannot do. A fairly commonplace condition, with no suggestion that it might affect branch accounts.	-
5.68	BrailsfordS2239K		1- hardware; pin pads	Typo in KEL id in Coyne report. Appears to be a fairly common fault in a PIN pad - fails to read characters correctly. No suggestion of impact on branch accounts.	-
5.69, 5.135	cardc219R		1- hardware; pin pads	A PIN pad issue connected with an older PIN pad (Hypercom) to be replaced by a newer one (Ingenico). The KEL suggests that the failure might lead to a failure to reverse a transaction. If this were the case, later reconciliation and a TC would correct any error in branch accounts - contrary to what Mr Coyne suggests. (UEC)	-
5.92	dsed4733R		3 - robustness	The failed recovery report showed a recovery which had failed, for a reason which was not entirely clear. Investigation showed it was caused by a mis-named recovery script. This incident appears to show that the robustness countermeasure of the failed recovery report was doing its job - allowing FJ to detect failed recoveries and correct them. (RDS, MID) Even if this robustness mechanism had not worked, the backstop of reconciliation and TCs would have corrected any remaining error in accounts. (UEC) So no impact on branch accounts.	-

FUJ00082226

5.93	obengc5933K		3 - robustness	This is further evidence of the failed recovery report doing its job - alerting FJ to failed recoveries, so they can investigate them and make any necessary corrections to accounts (RDS, MID) This was caused by a complex 'grey' communications failure which could not be reproduced - so diagnosis was not complete. Was this a failure of ROC in complex circumstances? The KEL gives no reason to suppose that, even if this condition had persisted, the backstop of reconciliation and TCs would not have corrected any resulting errors in accounts. (UEC)	
5.116, 5.118	wrightm33145J		4 (a) (b) (c) - multiple issues	This, and the next KEL, is the receipts/payments mismatch - analysed at length by Gareth Jenkins, and in my report - see above	
5.117	ArnoldA2153P		4 (a) (b) (c) - multiple issues	This is about withdrawn products, stopping rolling over. This effect would be obvious to the SPM (MID), and a fix was proposed (reinstate the withdrawn product, before the affected stock unit is rolled over.) (WOR) No impact on branch accounts	
5.118	ballantj1759Q	PC0194381	4 (a) (b) (c) - multiple issues	Lists 3 conditions which may cause a receipts/payments mismatch, referring to other KELs such as wrightm33145J. One is only in training, so has no effect on live branches. Acknowledges that these may need manual correction to avoid errors in branch accounts. As receipts/payments mismatches are very evident to the SPM (MID), any large one will get investigated and corrected - as GJ's reports imply. smaller ones (e.g. less than £300) may slip through.	some
5.120	acha1357Q	PC0208335	4 (a) (b) (c) - multiple issues	Complicated to analyse. A one-year effect, when the same TP came around again, after some products had been withdrawn. Peak created to fix it. Symptoms are obvious to the branch (MID), so in most cases the branch will ask for help and be given the workaround in this KEL, and in the next KEL acha3145Q (WOR). So only small occurrences can have financial impact, if the branch ignores them - or rather, chooses to take a hit in balancing and rollover.	small

FUJ00082226

5.121	acha3145Q	PC0198927	4 (a) (b) (c) - multiple issues	Cited in the previous KEL. A stock balancing problem (stock products - not stamps etc) but not caused by withdrawn products - caused by clerk doing some uncommon sequence. Will always be noticeable to the branch (MID), so this KEL gives detailed description of what to do (WOR) - and as the previous KEL, it is unlikely to produce errors in branch accounts. KEL says: 'Since this is a business issue, NBSC should be able to advise PMs of what to do'. So, it is not clear whether or not this was a bug. Check the Peak.	small
5.129	allend1645p	PC0209755	4 - data entry	Horizon UI allowed the clerk to do something strange - select 'Debit card' as a method of payment and start doing a debit card transaction, and later switch to 'fast cash' - i.e. a user error. Not preventing this may be seen as a weakness of the UI, as Coyne regards it - but not a serious one, as it was a rare form of error. (DUE) Did the Peak fix it? If there was any impact on branch accounts, like other user errors it would be corrected by a TC or monthly balancing (UEC) - so no impact on branch accounts.	-
5.130	acha621P		4 - data entry	An error in remming in was provoked by a rare sequence of events (outreach branch, system logout or inactivity logout before completion). Software error which was fixed - workaround in KEL before that. All remming errors produce a discrepancy between physical cash and Horizon cash, which gets corrected at monthly balancing or before (UEC) So no impact on branch accounts. JC comments about correcting branch accounts are therefore inappropriate.	-
5.132	EJohnson3937R	PC96606	4 - data entry	' Whilst remitting in currency it is possible to create a transaction with a positive quantity and a zero value ' See the Peak for whether it was fixed. A zero-value transaction has no impact on branch accounts. So, this weakness in the UI is an irritation for users, not relevant to the causation of shortfalls.	-

FUJ00082226

5.133	PSteed145J		4 - data entry	'Phantom sales' caused by hardware problems - fix by replacing hardware. Not a data entry problem. If not detected by clerk, might result in over-charging customer - not a loss to the branch	-
5.133	pcarroll1235R		4 - data entry	Instructions on how to deal with screen freezes. JC says 'it is not known how widely these were distributed to SPMs' - implying that they should have been. They were distributed to those who called for help, via this KEL. Since screen freezing is a rare problem, it is not obviously appropriate to send instructions to all SPMs - overloading them with information. If that was appropriate, why not send all KELs to all SPMs? No impact on branch accounts, any more than any other hardware problem. Horizon must be robust against these. (RHW)	-
5.136	jharr1323L	PC0254169	4 - transfer	Fishing rod licence request not sent to Environment Agency. Only detected much later. FJ only keep PODG records for 30 days, so could not check against what E said. I may agree with JC that maybe PODG records should be kept for longer, for better MID, BFC. Trade-offs? are PODG files very big? No impact on branch accounts - PO would need to send request to EA again. Attributing to the branch would be a back office human error, prevented by ability to read data that shows the branch did nothing wrong (RDS, SEK)	-
5.137	MArris3433I (no 46)	PC95051	4 - transfer	This was a software bug which allowed a transaction to be recorded twice after a session transfer. A fairly rare circumstance? Peak should record history of fix. Impact on branch accounts: as with a human error of recording a transaction twice, this should produce a visible discrepancy (either in cash, or in reconciliation with some client), which appears in a TC or at monthly rollover, and has to be corrected. (UEC). So, no ultimate impact on branch accounts, if the amount is significant (SPM may accept small amounts)	-

FUJ00082226

5.139	CharltonJ2752T		4 - transfer	Software bug in ADC scripts (reference data?), when user corrects an error using the previous key. Create wrong transaction. Fix quickly released to live - sounds like reference data (BFC). As previous KEL - wrong transaction produces a discrepancy in cash or client reconciliation, which needs to be corrected for monthly rollover (UEC). No impact on branch accounts.	-
5.141	SSur343P		4 - transfer	An error in network banking caused the customer's account to be debited although the TX failed at the branch. Cause not diagnosed so it was escalated at BIM. JC says it was an error in data transfer, and I agree. Poor ROC? Probably branch accounts were correct (no TX) - correction would require only central action by PO, in response to customer discovery. Only possible effect on branch accounts is if PO incorrectly attribute to branch error - very unlikely here, as PO realised it was not (RDS, MID)	-
5.142	LKiang3526R		4 - transfer	Similar to next KEL SSur5310P. Two authorisation agents active at once - only one should have been. Credited phone £10 twice. A back-end problem, outside branch accounts, which would need to be corrected by PO centrally, and would only affect branch accounts by a TC, if it were mis-diagnosed as a branch error. Because of extensive log information and diagnosis (RSW, MID) this did not happen and is unlikely. So, no impact on branch accounts	-
5.142	SSur5310P	PC103096	4 - transfer	As the KEL above. 'The cause is usually a network problem where there are delays between the auth agents and the correspondence servers. This may be because of maintenance work at a weekend....'	-
5.165	pothapragadac4359R	PC0208292 PC0209602	6 - bug fixing	Branches able to declare stock which they cannot transact - this might produce an error in branch accounts relating to those products. Two fixes were issued - see Peaks. Some impact on branch accounts cannot be ruled out, although it is small, because SPMs would note any larger effect and get it corrected (MID)	Small

FUJ00082226

5.165	Marris4123N	PC92832	6 - bug fixing	This was a problem observed in Disaster Recovery, for DVLA transactions - a very rare circumstance, which should be handled correctly, but nevertheless has no impact on branch accounts in routine use.	
5.186	acha2230K		6 - bug fixing	Two new checks have been implemented at the counter. This KEL is about how to respond if some SPM sees an alert raised by one of the checks and calls to enquire. It is not clear from the KEL whether any SPM ever had rung in about them. The new checks are to spot inconsistencies 'that should never occur' - and there is no evidence in the KEL that they ever did. Therefore, the comment from SSC in the KEL, cited by Mr Coyne, that 'This should never happen - something has gone horribly wrong' probably refers to a hypothetical situation, not to any real event. i.e. SSC mean: 'this check will only raise an alarm if something has gone horribly wrong'. See the KEL to understand this context. No impact on branch accounts, from extra checks in the system.	-
5.187	dsed2049S		6 - bug fixing	Many familiar elements - rollover, withdrawn products. Withdrawn products should be remmed out by the SPM (sent back to PO), so he is not holding stock he cannot sell. If he does not do this, he is left with a loss at the next TP rollover; the stock gets converted to cash, as if he had bought it personally. The reason for this was not clear to SPMs; a fix was made, to make it obvious to them. Any loss was fixable by NBSC; this KEL is to instruct the SPM what to do. Coyne implies this was a bug which took 6 months to fix. It was not; it was an improvement in the UI, to help SPMs who had made a specific error. One might claim the UI should always have done that (poor DUE), but it was a small UI issue. No impact on branch accounts - except possibly for small amounts where the SPM cannot be bothered and takes the hit.	-

FUJ00082226

5.189	acha3250R		6 - bug fixing	This was an issue with back end reports, caused by timing issues (APS transactions arriving a day late) which were outside PO/Fujitsu control. This caused discrepancies in certain reports, which could however be understood by looking at other reports (RDS, MID) This issue may, as JC implies, have complicated the reconciliation processes. A fix was considered but appeared too complex - a typical development trade-off. No impact on branch accounts, unless it forced some human error in back-end reconciliation processes, attributing some error to a branch. Because the problem was known and there were sufficient reports to understand its occurrences (RDS, MID), this is unlikely.	
7.6	acha1941L		14 - info for SPMs	The KEL says: 'This is not really a problem, it is just confusing when investigating a state 4 call. The Disconnected Session receipts will show all the transactions in the session. The successfully recovered transaction needs no reconciliation.' This shows that any misleading information went not to the SPM, but to someone in PO or Fujitsu investigating a state 4 call. The KEL is not relevant to issue 14. As there is no reconciliation needed, there is no impact on branch accounts.	-
7.7	surs1147Q		14 - info for SPMs	This KEL seems to be about SPM inability to log on in certain circumstances; it is not relevant to issue 14, reports available to the SPM. As JC notes, the advice to the SPM in the KEL is somewhat counter-intuitive, of the form 'do nothing; wait for it to time out" No implication of any impact on branch accounts.	-
7.9, 7.41	wrightm33145j		14 - info for SPMs	Yet another repeat of the same KEL above, involved in the receipts/payments mismatch; not clear why JC cites it here. He mentions prompts and warnings to the SPM.	
9.5	RKing5147Q		7 remote access Tivoli	This KEL is only referenced by JC in a footnote, and he appears to draw no conclusion from it, other than that Tivoli was in use, for remote control of branch terminals. No implication of any impact on branch accounts	-

FUJ00082226

9.12	boismaisons1328M		7 remote access	As with the previous KEL, this relates purely to the use of Tivoli for remote access to the counter. JC relates it to FJ's ability to access disc space sizes. Disc space sizes have nothing to do with branch transaction data, which in any case at the time (2012) was not stored in the branch. No implication of any impact on branch accounts.	-
9.13	acha2026Q		7 remote access	As the previous KELs, this KEL only supports the idea that Fujitsu could access the counter through Tivoli.	-
9.14	MillerK1837J		7 remote access	This is about providing help reference data to the counter. JC notes only that some of these files could be deleted remotely. This seems to be an obvious requirement for remote provision of help files and is not surprising. No implication of any impact on branch accounts.	-
9.49	SeemungalG519Q	PC0192868	7 remote access - TIP repair	About transaction repair, so may be complex and could possibly impact branch accounts. Investigate further.	possible
9.50	MHarvey2255P (no 64)	PC125333	7 remote access	About balancing transactions. Complex back end stuff, which may have impact on branch accounts. Investigate further.	possible

FUJ00082226

CHARTERIS

Appendix GG Mr Coyne's 8 KELs without countermeasures

221 The following table includes eight KELs, mentioned in the claimants' outline of 17th August. Therefore, I have had time to analyse them in more detail than other KELs mentioned in Mr Coyne's report - but this analysis does not include countermeasures.

FUJ00082226

KEL id, title and cited Peaks	Date	Extracts from KEL or Peaks	Analysis	Financial Impact?
		Range		

FUJ00082226

acha1233J Incorrect cash declarations received by Cash Management - errors relating to cash rem out PC0218835	6/12	The branch have been told by Cash Management that their declarations are very inaccurate, and have been so for several months, and they are not processing their remmed out cash correctly When the branch declare cash for each of their stock units, any cash in pouches should not be included. At the end of the trading day, Horizon adds together all the declarations and transmits them in a .coh file. This also includes a Generated cash figure, based on cash movements during the day, which does include Cash in Pouches. Information on cash movements into pouches (rem out), and pouches leaving branches (pouch collection), is included in the .ble files which are fed into POLSAP each night, containing all transactions done at the branch during the day, so POLSAP should know the balance held in pouches at the end of each trading day. The cash declaration received by Cash Management matched what the branch declared each day, and what was sent out of the Horizon system in the cash on hand file, EXCEPT for the £50 banknote (product 655). It appears that somewhere after leaving Horizon but before getting into the cash management system, an adjustment is being made to add the branch Cash in Pouches overnight figure to what they have actually declared. But rather than using the value for the correct trading day, it is using the value from the previous day. Hence the declarations being used by the Cash Management system do not match the cash actually in the branch. **From the Peak:** NBSC states has gone through all checks and confirmed the PM is following the right procedure and choosing the right dates. This doesn't sound like a Horizon problem - the cash on hand data is sent in the .coh files to POLSAP, and doesn't include cash in pouches. Details of pouch collection from branches are sent in .poc files. There must be a feed out of POLSAP into the cash management system (this information could also be based on financial data which we send to POLSAP in .ble files).	This appears to be an error somewhere between Horizon and POLSAP, so that POLSAP's record of cash remming in and out was incorrect - some entries had the wrong date. Cash Management depend on POLSAP, and therefore they thought the branch was doing something wrong. However, if the branch had done nothing wrong, their physical cash would match what was in the BRDB, and therefore there would be no imbalance for the SPM to correct at the end of a TP. If Cash Management had been sufficiently concerned to investigate the branch further, then examining the core audit records (which were not involved in the bug) would have shown that the branch had done nothing wrong. The effect of this bug was to raise unwarranted alarms in Cash Management, rather than to affect branch accounts.	No

FUJ00082226

acha1717T Branch reports an unexplained discrepancy PC0202239	7/10 - 2/15	The branch complained that they had a loss of £240 on one day. NBSC had been unable to find any reason for the discrepancy so the call was sent to Horizon to check for system errors. **From the Peak:** Cash was declared at 16:39 on Fri 23rd, with a discrepancy of -£40.34, and then at 12:20 on Sat 24th, this time with a discrepancy of -£240.66. I have checked very carefully between these times for any sign of a system problem, but everything appears correct. There were no timeouts or recovery. However I noticed session 2-751576, completed 16:51 on Fri 23rd. This session contained an A&L withdrawal of £200 at 16:46 and CAPO withdraw limit of £120.90 at 16:50, settled to cash £320.90. Given the gap between the transactions, I wonder if these withdrawals were done by two separate customers, and the first was given £200 and the second £320.90 (the stack total)? This would cause a loss of £200. I have spoken to the PM and explained there are no indications of any system problems, but this session could possibly be the source of the loss. She is going to investigate further and is happy for this call to be closed.	There is nothing in the KEL to indicate that this was a problem in Horizon - merely an unexplained error being investigated. The Peak shows that the error was investigated, by Anne Chambers.. No fault was found in Horizon. A possible account of the discrepancy was found, arising from a user error. The SPM was happy for the call to be closed.	No

FUJ00082226

acha621P Cash remmed in at outreach branch was recorded multiple times PC0246949	10/15-01/16	A cash pouch was received at an outreach branch and scanned into Horizon. The manual process was followed and 2 Delivery Receipts printed. Then the clerk pressed Enter to complete the process, and a Rem In slip was printed. They were then able to press Enter again and another Rem In slip was printed - and the same amount of cash was recorded a second time. They may have repeated several times before using Cancel to escape, resulting in much more cash being recorded on the system than they actually have. After the Rem In slip is printed, the Remittances & Transfers Home screen should be displayed. If there was a system logout or inactivity logout earlier, before the user had logged on fully and all the post-logon checks completed, then the Rem In screen is displayed again after the Rem In slip has been printed. The user presses Enter to try to exit; each time the pouch value is remmed in again. PC0246997: Fixed in CTR_APP_X1288_V646, released to live via COUNTER_APP 77_7. Roll Out to live estate commenced overnight Tuesday Jan 12th 2016. The cause of the problem is being investigated but it will not retrospectively correct the accounts at affected branches. **From the Peak:** This is not an area that has changed for several years so it likely to have happened before but we have no record of it having been reported to us. I can only check back two months; I've found 4 other instances (outreach branches 214869, 106444, 110444, 207828) and all but the last removed the discrepancy by completing a rem out for the excess, which corrected the system cash holding. Branch 224843 may be able to do the same but NBSC should advise on this. We are continuing to investigate the problem (PC0246997), but any fix will not retrospectively change the branch accounts.	This is a case where Horizon allowed a user to make an error remming in cash - remming in the same pouch several times. As a result, cash recorded in Horizon would not match physical cash. As above, when physical cash is counted and monthly balancing is done, any error will be corrected. So there is no permanent effect on branch accounts. The Peak implies that the problem may have been around for some time. Some SPMs spotted it and reversed the error immediately. Those who did not spot it would see the discrepancy later, when they counted cash, and have to correct it in their monthly balancing. Cash remming in and out must be proof against user errors	No
acha194L Kiosk cash declaration s failing PC0238702	11/14-02/15	A Post Office branch may report that cash declarations from kiosk(s) are not being automatically passed into the Horizon system so they are having to manually declare cash for the kiosk(s) directly onto the horizon system. Use of incorrect datatype can result in the Transaction Amount check failing when it is actually correct. Missing cash declarations from kiosks means no info is sent to POL about any cash held at the branch, and can impact cash management and deliveries. Though since kiosks declare a till within a shared stock unit, it is unlikely that all tills will be missing. Affecting around 15% of kiosk branches each day. **From the Peak**: Venu Anamalla Confirmed that this Incident may be passed to the external company with the attached evidence.	An error in Horizon failed to do something automatically. If the SPM notices, he can do it manually. If he does not, there is an impact on cash management and delivering cash to the branch. The business impact of the error is on cash management and delivering cash - that is, the cash needed at a branch may be incorrectly estimated, leading to late or insufficient deliveries. This is not an effect on branch accounts.. The Peak implies that the fault was not in Horizon, but in the kiosks managed by an external company.	No

FUJ00082226

LKiang3014S Cash declarations do not match Cash in the Trial Balance PC0084116	11/02-27	The system seems to be generating a discrepancy ("DDP -3438") that matches the cash declaration DecId rather than calculating it. Development have been unable to determine the root cause of this problem (PC0084116). Instead new trace has been introduced to Dataserver in BI3_S30. Now when Stockunit Balance reports are actioned all transactions trawled in are summarised whenever a search is requested. There will be a 'before' and 'after' trace appearing in the audit.log. If the cash in the Trial Balance is different to that declared by the PM and the discrepancy (which can be found by interrogating the Transaction Log: DDP or DDN) matches the last cash declaration figure then this could be the problem. A circumvention is to redo the cash declarations using the same amount as already declared. **From the Peak** Development have not been able to determine the root cause of this problem. But more trace message has been added to Audit logs in BI3_S30 for future investigations. However there is a circumvention (as described in KEL LKiang3014S) which is to simply redo the cash declarations using the same amount as already declared.	This was a problem in the monthly balancing process, which appears to have happened only once. After investigation, an extra check was put in the audit logs for future investigations, and I have seen no evidence of these Fujitsu could not find the cause of the problem ,and suspected a fault in the Riposte software. A simple workaround was suggested for any SPMs affected. Since the problem was obvious to SPMs if the amount was significant, and there was then a simple workaround, it is not expected to have significant effects on branch accounts. Small effects might not be noticed.	Small if any

FUJ00082226

MScardifield2219S Multiple cash declarations may cause incorrect figures in Discrepancy, Variance and Balance Reports PC121925	7/05-11/07	A cash declaration was made in "Stock Balancing" for the amount displayed on the Snapshot. When the Cash Variance was checked afterwards a Gain of £45.05 was displayed. **** May get PMs calling in to stating that they've been declaring cash but have been getting varying discrepancies reported even though they've been declaring the same amount of cash each time. Or that they have done a transfer but are then getting a discrepancy equal to the amount of the transfer, or that the system hasn't transferred the cash out of the stock unit. The underlying problem is that we cache the current trading position for a Stock Unit and rely on a mechanism (in Riposte) to notify us of new transactions across the outlet to keep this cache up to date. When this fails it affects Discrepancy, Variance and Balance Reports and has the effect of presenting the clerk with incorrect information. This will be potentially confusing and may lead to the clerk making unnecessary corrections. These will in turn show up as future inconsistencies (eg nothing gets lost in the end). The Declare Cash problem clears itself overnight. **From the Peak** I've added a sample trace file for one of the test rigs where over 17000 transactions were applied; if we multiply this up by a factor of 3 (number of days) times 3 number of rigs = 153000 transactions generated. Out of this I have seen ONE failure, so going on this statistic there is, obviously a 1 in 153000 chance of hitting this problem. Alas this problem is still related to some temporary resourcing problem (the one I wittnessed seemed to be down to a print preview lockup?), but the system did go onto recover but leaving the figures stagnant in memory.	The Peak implies that this was a very rare problem, which could only be reproduced with difficulty The KEL states that this problem may lead to the clerk making unnecessary corrections - which could lead to an incorrect cash position on Horizon. However, the KEL also says that ' These will in turn show up as future inconsistencies (eg nothing gets lost in the end).' This refers to the fact that nay remaining inconsistency will be corrected in monthly balancing, lending to a correct position.(countermeasure UEC)	No

FUJ00082226

wbra5353J HBS Error 1201 Invalid Basket State (state 4 DCP report) PC0233011	4/14	Review of the message log shows the session failed due to 'Invalid Basket state - error 1201' Thought to be a side effect of bad reference data for parcels to Singapore etc which was fixed on Tuesday 15th April. Therefore the implication is that a card payment has been taken even though the basket hasn't been successfully settled as it was subsequently cancelled. Or there may have been a subsequent successful settlement in the same session; check usage of the PAN on the DRS workstation. Call returned to MSU for progression with POL as to the way forward with reconciling what appears to be a fault with the kiosk. **From the Peak:** Note the repeated use of Sequence number 229 by the kiosk, which HBS has interpreted as a resend of a request and so we have effectively returned the previous response each time (though I see with the TransactionTotalRequest we call the response a TransactionTotalResponse which is not what I would have expected). This explains why we returned an error of Invalid Basket State to the first call of RTSTenderAdd. I see that there have been 3 attempts to settle this to Plastic. I?m not sure why you have allowed this, but it seems to have resulted in the customer having their card debited 3 times and the session was then cancelled.	This was a fault involving a kiosk, which resulted in a customer being debited three times, after CHARTERIS which the session was cancelled. This would be a recoverable transaction because it involves a credit card; cancellation and subsequent recovery would lead to no net effect on the branch or the customer. The fault appears to result from two causes: (a) bad reference data, which was easily corrected, and (b) a fault in the kiosk software, which came from an external supplier, and was outside PO/Fujitsu control.	No
jsim5530K Remmed out cheques twice by mistake and unable to reverse PC0203153	8/10-10/10	PM states that she remmed out her cheques twice by mistake so she spoke to the NBSC who advised her to reverse the addtional transaction session by doing... BackOffice > Admin > Reversal > Existing Reversal When the PM attempted this the following message was displayed... Reference data controls which transaction modes may be reversed, in this case the reversal of a cheque rem out transaction is not allowed. The reference data is controlled by the Post Office so this is a business issue to be progressed by the NBSC.	This condition (not being able to reverse a mistake) is visible to the PM, and leads to a discrepancy between Horizon and reality in cash + cheques -just like many other human errors in handling cheques. Monthly balancing will show a discrepancy, which the PM will understand, and correct the error. It is not recorded whether the reference data was changes, to allow a double rem out to be reversed.	No

FUJ00082226

Appendix HH My 50 KELs without countermeasures

222 This table contains a further sample of 50 randomly selected KELs (also every 100th KEL in an alphabetically sorted list) which I have analysed for possible financial impact - but I have not analysed them for robustness countermeasures.

FUJ00082226

KEL id and title	Date	Range	Extracts from KEL or Peaks	Analysis	Financial Impact?
JBallantyne4231Q MAESTRO job DRS_EFT_C12_PARS.DRSC312E did not die	2/05		Having looked at the module, what it does is when it sees the C12 parser has been stopped, it goes and checks for one last time for any new transaction and failure counts and updates the "Monitor" table before exiting with success. So the module wasn't hanging it was just doing the final processing for the day.	Maestro is a job scheduler, so this was a back end performance issue - jobs running too slowly, but correctly - which would have no influence on branch accounts.	No
jenningse2856P Audit - QueryHandler.exe running at 100% CPU usage	10/09		the result was that the QueryHandler.exe was running at 100% CPU usage affecting the platform performance and causing an upgrade to fail (due to a locked DLL). Believe that something had happened to a particular (BRDB orientated) ARQ.	ARQ is a process for retrieving audit data, and has no effect on branch accounts	No
jenningsg4223J R12.01 - samba log guest user Access denied on IPC$	3/15		On the new V2 platforms Access by the Archive servers to the MAEARC$ share via the audit external user is generating a symbiotic error for guest user to the IPC$ share (which does note exist in the smb.conf). 2 x errors per platform are generated every day at approx 14:00 when the B_AUDIT_STRT1.MAES_AUDITB and W_AUDIT_STRT1.MAES_AUDITW jobs kick off at 14:00	Samba is a unix program that allows filesystems exported from Unix hosts to be mounted on Windows systems. This is a back end access issue. Access to these logs is very remote from branch accounts - no effect.	No
JonnalagaddaN236N Time synchronization Error	3/11-8/17		Attempt to set time which differs by more than 12 hours aborted. If no event seen, SMC need to raise a P5 call and pass it to HNG NT team (Platform Owner / SDU) team to restart the windows time service, no need to contact on call out of hours, an email to our team mailbox will sufficient .	This is a back end server problem, and there is no evidence that it has any impact on branch accounts. Horizon has to be designed defensively, so that a back end job being aborted for any reason (such as a hardware failure) will not have any effect on branch accounts..	No
jsim255Q BPOSRT201101BranchOrdersYYYYMMDDHHMMSS.xml moved to failed directory	10/08-2/11		These are Bureau Pre-Order APOP reports that are created and sent to EDG every 15 minutes. The Peak PC0167591 established that this was a	This was a fault in producing a report file to a client organisation (First Rate). It seems to have happened only occasionally, and the	No

FUJ00082226

	1	problem with sending foreign exchange transaction data to First Rate: Transactions will be posted to APOP with a status of Paid. · The APOP SQL Extract process will run on a 15 minute cycle throughout the working day, to produce a file of records with a status of Paid and to change the status of extracted records from Paid to Available. The SQL extract will produce a file in XML format. · The APOP FTMS service will make files available to EDG · EDG will forward the file to First Rate via SFTP · First Rate will process orders placed before 2pm on Day A, shipping currency / travellers cheques for the Customer to be able to collect from the originating branch on Day B. Orders placed after 2pm will be shipped for collection on Day C. Therefore it would appear that First Rate are the customer in this case. The final status was ' Closed -- Advice after Investigation'	solution was a manual re-send of the file. Even if there had been any impact on branch accounts (which was not evident from the Peak, and which is ulikely), later reconciliation with First Rate would have corrected it	
JSimpkins4251P "Migration Special" required for missing products	9/99 - 01/00	During the migration of a new counter it was found that non-core items used by that office were not available at the counter Some reference data has not been provided by POCL to activate those products at this office.	Some products not being available does not lead to errors in branch accounts.	No
KalagampudiS1911J CRON 100 : pmcc_collect: ERROR: start_collection returned error code 60	10/15	These errors were caused by the builds of lprpbsl301+302 enabling pmcc data collection from all 4 arrays. This put extra load on the arrays and interfered with the collection from the current servers, lprpbsl201+202. Unix team have now disabled the collection on BSL301+302.	This was a back end batch performance problem. The link to branch accounts would be very indirect, and there is no evidence there was any link	No
KalagampudiS5733K PI11NSW004 sent to neighbor 192.168.21.2 4/0 (hold time expired) 0 bytes	9/13	There is little in the KEL beyond the title. ' PI11NSW004' is a network switch - see document 138062002.	A problem with the data centre LAN is very remote from branch accounts. It might interrupt some processing, so some applications might have to recover, and must be designed to recover from network hardware faults.	No
KennyA2520K iKEY locked out after Password change	6/10	Changed the iKEY password unable to log on. Send iKEY to Bracknell for RMGA Security Ops to rectify problem.	RMGA = Royal Mail Group Account People being locked out of applications - for instance, because they have lost their	No

FUJ00082226

		RMGA security may take actions defined in local work instructions to allow temporary access.	password - is a regular event, and delays processing rather than introducing errors. Systems must be designed to be robust against the introduction of errors.	
kiangl230J TivoliServiceMonitor:Service Not Running - TMSIPPSA - Restart Count Exceeded	4/14-2/15	It seems that the composite product COUNTER_X1005 failed to install AGT_IPPSA correctly. IPPSA is the Ingenico PIN Pad Serial Adaptor Agent introduced on Counters to enable ARC (Asylum seekers Registration Card) processing. If the counter keeps throwing this alert and it needs to be resolved then a counter replacement can be requested. There are other ways of re-instating, but, according to Dev, they are tricky and un-tested, so replacement of the counter is the safest option.	This is an inconvenience that stops counters processing some kinds of transactions (ARC), but does not introduce any error into branch accounts.	No
KrishnaC2131K CIT R5 Drop 3c CTR_05_0_3_63 - Recovery successful when ADC Recov script fails to compile	7/11	PM performed APADC recoverable transaction and added the transaction to basket and counter got crashed due to some problem and settlement didn't happened. At the time of counter recovery process, APRecovery got kicked off and attempted to execute ADC recovery script which has compile error. Then counter displayed compilation error message as expected and pressing continue over that printed recovery successfull receipt, which was wrong. From the Peak PC0210980: What live problems will there be if we do not issue this fix? --If the fix is not released, recovery failure due to script failure, adds a dummy line to basket and prints receipt as recovery success and misleads user as recovery happened, but in actual it didn't happened.	Issue was a recoverable transaction, and may have caused an error or induced the PM to make an error. Human errors in recoverable transactions are quite common, as the recovery process is not routine. Recoverable transactions only need to be recovered because a 3rd party client is involved. If the SPM is misled or makes a mistake, reconciliation with that client will correct the error .	No
KumarR2346P Missing Time To/From Criteria when Building Transaction Log Query.	6/11	If you enter a "time from" or "time to" value when setting criteria for a transaction log report, then the values entered disappear from the transaction log history as you enter more criteria.	This may well be a report for an SPM in a branch - I need to check. Generally, errors in reports to SPMs do not directly influence branch accounts. If a misleading	No

FUJ00082226

			report induced a PM to make an error, then monthly balancing would generally correct it.	
LeavesleyC5224K (103) Horizon_Remove - failed to delete folder C:\cryptography\RecCode	3/11	Event text: (103) Horizon_Remove - failed to delete folder C:\cryptography\RecCode Severity: Critical Alert group: InstallSW From the Peak PC0209342: Since the messages in the app event log and the entries on the Tivoli website both indicate that the installation succeeded anyway, and there are no other associated errors, these events can be ignored.	This was an application installation problem, which has no direct effect on branch accounts. As the Peak said the events could be ignored, the impact seems to have been no more than a misleading message.	No
mansfielda2957Q PODG attempts to continue processing a file after a virus check failure	02/13	If a file arriving on the PODG external server is found to contain a virus, messages similar to those below will be logged to the application log: .... A spurious message stating 'An attempt to move the file failed' is logged because PODG continues to try to route the file even though it has been moved to the quarantine directory.	A spurious message in a log will not affect branch accounts	No
maxwellg251H BRDB_TA_FROM_TPS.BRDBX003_TA_FROM_TPS_n Abend	08/11	An attempt to load transaction acknowledgement data from TPS to BRDB has failed. The "ORA-00001: unique constraint (OPS$BRDB.TTAD_PK) violated" errors occurred because a transaction acknowledgement file presented to Fujitsu by Logica contains reference values which already exist in BRDB, or contains more than one entry with a given reference.	This problem was not caused by any defect in Horizon. It was caused by a fault in a file sent to Horizon by a client (Logica)	No
maxwellg85I Critical DCOM Event Id 10005		Event description - DCOM got error "The service cannot be started, either because it is disabled or because it has no enabled devices associated with it. " attempting to start the service SENS with arguments "" in order to run the server {D3938AB0-589D-11D1-8DD2-00AA004ABD5E} The event can be ignored.	DCOM is probably the Microsoft Distributed Component Object Model.It is referred to in 138061661 ' Proactive Monitoring Unix Supporting Agents ' As the KEL says ' the event can be ignored ', there is no expected effect on branch accounts	No
MHarvey1422M SSC_BO_GATH.SSC_BO_DRSSUP is overunning	12/03	SSC_BO_GATH.SSC_BO_DRSSUP schedule was overrunning because all files in m_db_srv:/bvnw01/drs/trans/drssupport dated 29 and 30th December were timing out with "file in use by another user" while attempting to copy to MBOSSC01\repository\host\drssuppo	This is a performance and scheduling problem at the back end. These may occur fairly frequently and there is no known link to branch accounts.	No

FUJ00082226

		The problem is not fully understood but was eventually cleared by a reboot of MBOSSC01. This appears to be an isolated incident and a reboot is probably the simplest resolution if only one client is affected, however if it occurs frequently then might be advisable to ask ISDNT to advise on how to get some diagnostics		
MithyanthaJ2129R Counter APP - Exception whilst executing action - java.lang.NullPointerException	4/10- 3/11/12	The error "Exception whilst executing action - java.lang.NullPointerException" will occur due to various reasons during the run time of the application. In this call, java.lang.NullPointerException occurred within Post Mail Items whilst the PM was messing around with postcodes. "MSG90025: System Error - Error Code: 0291" was displayed. The Peak was categorised as closed, and non-critical.	The KEL and the related Peak are rather unsatisfactory, as a Java null pointer exception can arise for a wide variety of reasons, and will generally stop a program from doing what it was doing. The KEL: and the Peak do not identify the root cause. The description of the activity taking place, 'messing around with post codes' seems to be detached from any business transaction, so it is unlikely to have any effects on branch accounts. Had this condition occurred with any significant frequency, Fujitsu would have had to investigate it further. The fact that they did not implies that it was an isolated incident.	No
mudundis3439Q Counter froze while settling Local collect Release and Return items.	3/11/10-	User is getting logged out automatically. The same barcode is used for Release or Return without getting settled during Accept(still in Basket). It is throwing unique constraint (OPS$BRDB.BPB_PK) violated as it is trying to update two states into a single cell as LCIn and OutOfOffice state at same time. PC0202466 - I spoke to the PM at the branch that was generating this event, who told me they weren't experiencing any operational problems. PC0205976 sent to 4th line as this problem is seen in live regularly, and it should be considered for a low priority fix. PC0205976 says: For the previous Monday and the Tuesday there was 1 branch that featured on both days 137002 so I had a look at the logs for the Monday and this shows a Consignment to Austrailia with 6 bar	The Peak directly referred to arose in testing, not in live use. However, the two other Peaks do refer to live use, and contain advice to SMs to avoid the problem. Counter freezing can arise for a variety of reasons, and the system must be designed so it has no effect on branch accounts. PC0205976 illustrates that the effect is an annoyance to the SPM - freezing, requiring a workaround- rather than an error in branch accounts. A low priority fix was required. Had there been any impact on branch accounts, it would have been high priority.	No

FUJ00082226

		codes scanned, then a UK packet no othere services selected but the reciept contained a Barcode that was scanned in the consignment this is unexpected and possible cause of the key violation. Althought this may be environmental the code needs to be robust enough to avoid such instancies. This can be scheduled as a low priority fix. Attaching logs for 137002.		
MWright454P Errors in Stock Unit Deletion messages	1/02- 1/ 0 3	There are two User Maintenance/Stock Unit/Delete messages that appear to be hard-coded. The first one is displayed if a stock unit has pending transfers. 'Stockunit' (all one word) needs to be replaced by 'stock unit'. The second needs to be changed by removing the text 'ATTENTION Counld not delete stock unit SS as' so that it matches the other message. It then becomes: Stock unit nn counld not be deleted – it has been used in the current Cash Account Period. This issue is having insufficient effect on the live estate to warrant the investigation of the fault and production and application of any subsequent fix. Should the problem recur and prove to cause a major impact on either the support community or the end user then the status of this fault will be reviewed.	This was a cosmetic user interface issue - no impact on branch accounts. There was 'insufficient effect on the live estate' to warrant further wrk.	No
NarayanS1133K Windows cannot find the machine account	8/11	Server Name : LPRPBPL001 Event Text: Windows cannot find the machine account, The clocks on the client and server machines are skewed. This alert is triggered during the BPL server reboot which takes place overnight.	Being an overnight event on a server, this is a back end issue which takes place outside business hours. Therefore any connection to branch accounts is remote.	No
NStreeter1458Q All Users at PO unable to change SU Attach Button Grey	6/00- 1/ 0 3	All counters and all users were unable to attach to a different Stock Unit. The attach key is greyed out and the F3 key does not work. The problem is caused by a corrupt stockunit object in the message store, it will be missing items when compared with other stock unit messages. This causes EPOSSStockunits.dll to fail and makes the Attach and F3 keys unavailable.	Inability to attach to a different stock unit will prevent users from entering any business transactions or roll over the stock unit, rather than allow erroneous transaction to take place. Therefore there is no effect on branch accounts. (check the Peak)	No
OAgboola448S The file system / polfs/ads has reached capacity of 96 % on sbosap01A	8/05	The file system has reached a near full capacity on the server, and has taken almost all the spaces up on the said server. A basic housekeeping activity deleting irrelevant files should resolve this.	This is a back end server performance issue, and has no effect on branch accounts.	No

FUJ00082226

P.rose5349G Error Encountered	7/03	Critical Error: 'Error [condition encountered] Function:clsPANH'.	Very little evidence provided in the KEL. Need to see TFS 307211017	No
PawasheC4544Y APS2 Session 330 is blocking 30 other sessions	12/09	Server : LPRPOES001 Date / Time : 27/11/09 20:15:26 AlertKey : APS2 AlertGroup : OEM Alert:- Summary : APS2 Session 330 is blocking 30 other sessions. This is something that occurs at the same time as the TPS Hydra feed it doesn't cause an issue, so can be ignore this alert between 8pm and 11pm each night.	This is a server issue which the KEL says 'can be ignored'. So there is no effect on branch accounts	No
PCarroll4137R NT Polo Reset does not work on Gateway	11/00	VPN does not get initialised until Polo has completed. See KEL GCritchley4855L.htm for a full explanation. If and only if this is a CI4 gateway system, then Box Swap is the only answer. The referenced KEL says: Counter has been rebooted and it has presented the normal Windows NT logon box - instead of the Polo login screen Replace the offending unit. Obviously care must be exercised to ensure that all transactions are up to date otherwise we may lose some!!!	This raises a risk of human error (not ensuring that all transactions are up to date) when replacing a unit. In that case, the usual methods for correcting human error (monthly balancing and rollover, transaction corrections) would apply. So there is no potential for introducing permanent errors in branch accounts.	No
PorterS2059K CounterApp Windows NT Alert 0221.reference.data.local.checksum.mismatch	02/12	Clerk may not be able to log on to the Counter as the CounterApp refuses to appear on the screen; Counter desktop is blank	This causes the counter to be unable to process customer transactions, but does not introduce any erroneous ones.	No
PSteed3244P TPSC268A: Reversals for end-dated products are not included in Host figures	6/02- 5 / 0 4	Detailed description of symptoms. This is a reporting error. Cash account produced at the counter is fine. It's just the host processing that is at fault May 2004: The solution to this problem, detailed above, has been reversed by the fix to PC0097511 (KELs AChambers3558R and DSeddon3616K). If there are regular occurrences of this problem then we will need to think about getting it looked at again by development.	'Host figures' refers to a back-end reporting problem. Since the cash account produced at the counter is correct, there is no adverse impact on branch accounts.	No
RAloneftis5111J	8/05	Call raised by EDG as the Bureau De Change Margins file received .MRG (BDC-M)contains incorrect	This problem seems to be a delay in producing a report at the back end or for a client. This	No

FUJ00082226

Problem with BDC-M file header marked as being for a future date		information and sites are trading with the incorrect price groups. Following investigation by Unix the file received on that particular day contained an incorrect Header which instructs RDMC to load the file on 30-JUL-2005 which is a date in the future. The file has been placed in a "WAITING" directory, and will be processed by approx 08:25 tomorrow morning.	has no impact on branch accounts.	
RamaswamyP4748M (60) ATE Summary page & ATE Status page is not opening	6/09	ATE Summary page & ATE Status page is not opening in Tivoli Web Pages. This problem will not be resolved under Horizon (it is more than likely a issue with the version of IE 5.50)	ATE = ? 'Tivoli web page' means that this issue is connected with Tivoli distribution of software updates, not to do with business transactions. Internet Explorer 5.50 is failing to display some information, and there is a workaround. Therefore the connection to branch accounts is very remote.	No.
RColeman4719K Boot server: CreateFile and ReadFile failed events	01/03- 0 1 / 0 4	Events on Boot Server: Event ID: 2002 "CreateFile (cfg pipe create) failed." Event ID: 2003 "ReadFile (cfg pipe read) failed. The ConfigRequestHandler service uses a pipe to pass ISDN details to the FindDtls program. Without this pipe Boot Server Files will not be processed when a FAD dials in. Stop and start the ConfigRequestHandler on the affected Boot Server. If this does not work then reboot the Boot Server.	The Boot server is used to configure Outlet PCc during the installation process.. (doc 138140413) Therefore this fault would lead to difficulty setting up a counter PC, rather than any inaccuracies in branch accounts.	No
renwickh411K ORA-00257 alert being seen on various platforms/ events	12/10	Received minor alert @ 13/12/2010 17:35:07 on WSYSINV102 Event Text: The E: disk is at or near capacity. You may need to delete some files. IBM stated:- This is an Oracle error that indicates the disk where Oracle writes its redo archive log is full and the archive process is stuck. To resolve this problem, free up space on the disk where the redo archive logs are stored. Do not delete logs that have not yet been archived since you would	The reference to Oracle shows that this is a back end issue. It is an operational issue of keeping the back end systems running, rather than anything which could corrupt branch accounts. Horizon must be designed so that operational problems like this do not threaten the integrity of branch accounts.	No

FUJ00082226

		not be able to recover transactions in those files if your database were to crash.		
RKing212D SERVER Monitors: BAD Alert Shows For 1 MBODCA0<n> High Level Monitor For ETXCONFRT<n>_0_ISC Monitor.	11/03	A Real Time E-Top Ups Expedited Confirmation TMS Interactive Agent on one of the Bootle DCS Authorisation Agent Servers is not running for some reason.	This is an operational issue of keeping the back end systems running, rather than anything which could corrupt branch accounts. Horizon must be designed so that operational problems like this do not threaten the integrity of branch accounts.	No
RKing4032H CRITICAL Service Monitors. Monitor(s) Showing Bad Alert: ETAUTH0_<B><W><n>.SERVICE.	11/03- 5 / 0 5	This Monitor shows a BAD Alert if the DCS Authorisation Agent Server is unable to provide the E-Top Ups Authorisation Service.	Another operational issue, which is very unlikely to affect branch accounts. May stop branches processing some types of transaction, but not process them incorrectly.	No
RKing5642K LPRPPLG001: 'Soap errors' events raised (Track and Trace agent)	10/05- 2 / 1 8	Soap errors generated on LPRPPLG001 indicating issue with connection to 3rd party Track and Trace / SmartPost / RMGTT(Mainframe) service run by 3rd party/ ATOS SOAP errors in this pattern indicate an issue with the Track and Trace Interface (TT_Inf) agent connecting / passing requests to the 3rd party. This may because of persistent problems in the network between the Agent and the EDG / EDG Web Services layer, OR because of problems at the EDG / EDG Web Services layer. PC0210096 is being investigated to see why we do occasionally get a set of these errors (usually 4, but could be up to 160 all within a second or so) but investigations so far suggest this is just a transient failure and the soap messages are resent successfully.	This is an issue with web services connecting to client systems. Therefore its maximum impact is to prevent branches processing scertain types of transactions, rather than to process any incorrectly. No impact on branch accounts.	No
RRoll2214P Critical Error 2045 'sub RespondToBootRequest ... %9999	01/03- 0 1 / 0 4	During rollout of new counter (counter increase) the counter red screened and the folowing error was seen in th event log: Unrecoverable error no. 2045: 'sub RespondToBootRequest: Counter PC has an unexpected bar code.'.%9999 Please contact your support desk Reboot the gateway PC. If this does not work contact SSC.	This fault would temporarily prevent a new counter from operating at all, rather than make it operate erroneously.	No
SBullen821S	3/06	Interstage server was unable to terminate the DVLA Service work unit, which was restarted by the server.	This appears to have been a one-off event.	No

FUJ00082226

INTERSTAGE unable to terminate Reason Code (30)		All OK. Confirm that restart event has been seen. If persistent problems then further investigation recommened.		
SekarK5025D ORA-29283: invalid file operation ORA-06512: at "SYS.UTL_FILE", line 488 ORA-29283: invalid file operation	3/10-1 2/1 0	As informed by SSC, The exception was caused by the Transaction Correction Tool (BRDBX015) not having permission to read the input file. The exception can be ignored.	This was aback end server issue, involving an exception message which 'can be ignored'. S there is no expected impact on branch accounts.	No
ShenoyG4856U CRON 100 : latch: shared pool average wait time is 170	02/10	Very little further information in the KEL.	There may be some information in the TFS. This appears to be purely a performance issue, with no impact on accounts.	No
SParker1754N VPN key negotiation events	04/00-0 1/0 0/0 4	Event ID: 4006, Source: VPN Keymg, Key set for IP address nnn.nnn.nnn.nnn which belongs to /C=44 /CN=F /STA=65535 /L=P /PN=1000. (Acceptor) Event ID: 4006, Source: VPN Keymg, A key negotiation was started by nnn.nnn.nnn.nn These events are expected and can be ignored.	Events can be ignored - no impact on accounts	No
SParker957I The description for Event ID (nnn) in source (xxxxxxxx) could not be found.	01/01	When viewing event logs on another system the folowing is displayed in the event text:- The description for Event ID (nnn) in source (xxxxxxxx) could not be found. It contains the following insertion strings....	A minor problem viewing event logs - a record of past events - will not impact branch accounts	No
Stephensonm5042R SNMP Service Terminated Unexpectedly. It has done this 15 time(s).	04/06	Very little detail in this KEL	May be more in the TFS. SNMP = Simple Network Management Protocol Appears to be an operational network problem. Horizon must be designed to be robust against these.	No
surs2432R Failing to download Helpfile refdata	02/10	PM states that she has system freeze/slow on node 2 Checked the event log and noticed the that the counter was failing to download the Helpfile refdata and retrying after 15 minutes. This download process was carrying on throuth out the business hours. I suspect this has effect on counter performance...	A counter performance problem does not result in faulty accounts.	No
SwamiG2738R The driver has detected that the multipath group	7/16	The events triggered as a result of a MSC being actioned to presented new disk drives to the servers.	This is an operational back end problem, and is expected to have no effect on branch accounts	No

FUJ00082226

associated with LUN UUID				
TatugutlaP3518J The Network Connection Broker service terminated	2/18	Server: LPRPKSN202 Event Text : The Network Connection Broker service terminated with the following error: A device attached to the system is not functioning. Issue with User user logging off the workstation locally. Single instance of this alert can ignore.	This is an operational network problem at the back end, with no impact on accounts. It was classified as 'can ignore'	No
TurrellC2435P HNGX New branch fails to open	11/10-4/14	Engineer on site to open a new branch but the office is unable to rollout. Complex discussion of how to work around the problem.	Failure to open a branch simply stops it doing business, rather than making errors in its accounts;	No
VictorV1636P SMG_Execute_Tripwire_Client - Software Integrity Check failure. A copy of report C:\Program Files\Tripwire\TFS\report\LPRPDEA001-20091105-200204.twr has been sent to the DIAG server.	12/09	This was under investigation and not resolved.	There was some problem checking the integrity of the software on TFS. Little is known about it. Need to look a t the TFS	No
vincentn3446M APEX RDDS Exception HNGX004 HNGXMemoMonitor Failed to open cursor cur_NEWMEMOS	11/09-12/09	HNGXMemoMonitor on RDDS was trying to open a database link to RDMC; this was failing from once every few days to twice in one day. This procedure is run every few minutes, so the business impact of an occasional failure is very low.	As business impact was reported to be low, expect no effect n branch accounts.	No
vincentn849L PAM: Authentication failed for illegal user root	09/12	Secuirty events seen oon LPRPRSH003 RDT Solarios Server Events as a result of Patching work being carried out on MSC 043J0345812-02 Title: EXPEDITED - Applying Manufacturers Security Patches in the form of Baselines to the RDT Rig. Contents to be provided by Release Note once available from Release Management.	A back end operational problem. No evidence it had any impact on branch accounts. Check TFS	No
wbra3336L ALL users unable to log on to TPM / WAS service hangs.		When accessing TPM ( ) all users presented with: Invalid username or password. Re-enter the information and click Log On. for ALL users Looking at the log on /opt/sysmgt/logs/tpm_process_check.log can see that the service failed due to lack of space. This was tracked down to the housekeeping failing on the daily backup. These have been tidied and the DB2 and TDS services restarted (akin to a reboot without taking down the	An operational back end problem which was solved.	No

FUJ00082226

		server).		

CHARTERIS

FUJ00082226

Appendix II CLAIMANT ANALYSIS - DETAILED MATHEMATICS

FUJ00082226

Appendix JJ ANALYSES NEEDED IN SUPPORT OF MY OPINIONS

FUJ00082226

Appendix KK SAMPLE PEAKS AND KELS

225 The purpose of this appendix is to substantiate with evidence how Horizon incident management works in practice by examining sample Peaks with their corresponding KELs. My emphasis here is on the processes used, rather than the substance of the problems.

Appendix LL Peak PC0202239

226

227 The call was opened on 29 July 2010. The SPM had rung the NBSC to complain that they had lost £240. NBSC was unable to find any reason for the discrepancy so the caller was referred to Horizon to check for system errors.

228 The call was taken by 1st line support, who checked the event logs for any sign of a system problem but found none. It was then referred to 2nd line for deeper investigation.

229 The investigation was carried out the following day. The most likely explanation of the loss was that the customer in question had inadvertently been given too much cash. The investigator called the SPM and explained there were no indications of any system problems, but the customer session could be the source of the loss. The SPM was going to investigate further and was happy for the call to be closed.

230 KEL acha1717T was raised on 30 July, as the original call was closed. This includes a description of the problem and possible causes, and advice to the various support teams as to how it should be investigated and solved in future. The following extract illustrates part of the advice:

'**SSC:** Ideas for investigation:

- Have they Declared Stock by mistake? (see KEL acha3145Q)
- Use SmileyDesktop[21] Declaration Events, to find Declarations and Variance Check messages (the latter only if the PM uses the Variance Check button or an individual stockunit. May be some entries for stamps too). This may indicate a day where there is a significant change in discrepancy. On the other hand, many branches frequently have big differences between the declared cash and what the system expects them to have, and we have no way of knowing if there is a good reason for it or not.
- Use SmileyDesktop Session Data by Product, for product 1, to get all cash lines for the Balance Period. If you sort this in date order with the declaration events in a spreadsheet, you can calculate the system cash position after each transaction since the period start, and confirm that the variances / discrepancies reported are correctly calculated.
- Check with MSU (or check on Peak) whether there have been any reconciliation calls relating to the branch.

21 A support tool written by Fujitsu

FUJ00082226

- Check the application event log for any log4j events. Timeouts or IOExceptions may indicate problems contacting the data centre, and could have resulted in confusion with incomplete sessions / recovery. Check session data / recovery data / rep events / postofficecounter.logs to see what happened.
- Investigate any other unexpected log4j events
- See KEL acha522T for a user error that can cause a loss.
- Check for withdrawn products that have been converted to cash (see dsed2049S)

When responding, if they have given specific examples that you can explain, do so; otherwise make clear it is not a system problem (assuming you have checked that everything adds up). See PC0229446 for an example response which may help with the wording.'

231 Note that this advice refers to three other KELs (including dsed2049S) and a Peak (PC0229446), which may help agents to formulate the wording of the response to SPMs.

232 In my opinion, this example demonstrates an effective support process:

- The original incident was investigated and resolved promptly.
- The knowledge base was enhanced, taking advantage of earlier entries and other existing documents.

Appendix MM Peak PC0195672

233

234 This call was opened on 05 March 2010 as a result of testing on Postal Services. The user was incorrectly logged off by the system after accepting barcodes. When the user logged back onto the counter, the system recovered successfully. Therefore, this fault was merely an annoyance with no impact on branch accounts.

235 KEL mudundis3439Q was raised the same day to provide advice in case this problem occurred on the live system.

236 On 08 March, the Peak records that the QFP (Quality Filter Process) review was complete.

237 Preliminary investigation determined that the problem was transient and not straightforward to reproduce. After consultation with the Design team and a system architect, it was attributed to an environmental problem - i.e. caused by a specific set of local circumstances, which would not apply most of the time.

238 On 03 August, Peak PC0202466 was raised to investigate an automatic critical alert from the live system. The symptoms were immediately matched to KEL mudundis3439Q, discussed above. When the relevant SPM confirmed that they were not experiencing any operational problems at the branch, the Peak was closed on 09 August.

239 Peak PC0205976 was raised on 01 November in similar circumstances to the previous Peak. The new Peak records that 'Progress was delivered to Consumer', although it is not clear from the evidence that I have seen what the user's experience of the issue had been.

FUJ00082226

240 By 04 November the problem had been investigated in the light of the previous two Peaks identified above. The investigator saw the need to improve robustness and concluded:

'*Although this may be environmental the code needs to be robust enough to avoid such instances. This can be scheduled as a low priority fix.*'

241 In due course, according to its low priority, a fix was developed, tested and rolled out on 03 May 2011. The corresponding Peak was then closed.

242 The original Peak PC0195672 was finally closed on 29 November.

Commentary

243 This example shows the value of Horizon's service management processes and their associated records, stored for example on the Peak and KEL systems:

- The record of a problem originally observed during testing was used to inform the investigation of two live incidents.
- Both live incidents were detected through active system monitoring
- A wide range of expertise was brought to bear on what was a relatively minor issue.
- Because the software fault had no major impact on SPMs and certainly not on their accounts, it was treated as a low priority, which was nevertheless eventually fixed.

244 In my opinion, Horizon's support records are fit for purpose and compare favourably with equivalent documents that I have seen for other systems.

FUJ00082226

Appendix NN DETAILED RESPONSES TO MR COYNE