

RISKS RELATING TO UNIT HOLDING REGISTER AT RANDOMCORP

CONTEXT

The purpose of this document is to identify, analyse and recommend treatments for risks associated with errors in the unit registry in RANDOMCORP.

It is prepared in the context of the Enterprise Risk Management system recommended to the RANDOMCORP board in Assignment 1.

WHAT IS THE UNIT REGISTRY?

The unit registry is a database that is used to administer the unit holdings of individual investors in RANDOMCORP's pooled unit trusts. It keeps a record of the people investing in an investment and the number of units they hold.

Pooled unit trusts are a common investment vehicle in Australia and work as follows.

- An investor purchases units in an investment vehicle at the going price for the units at the time of purchase.
- The investor's money is then pooled with the money of other investors and invested in assets on the investors' behalf by an investment manager.
- Units then increase or decrease in value over time; and the investor eventually cashes in the units for the going price at the time of sale.

More information on the operation of unit trusts can be obtained from the Unit Pricing Guide, jointly prepared by ASIC and APRA (see the references at the end of this document).

WHY IS THIS IMPORTANT?

Errors in unit pricing and allocation are rare compared to the number of allocations made each day, but are a substantial risk to Financial Service organisations like RANDOMCORP. According to the Unit Pricing Guide, the cost of some errors has been greater than \$10 million.

SCOPE AND PURPOSE

There are many potential causes for errors in unit pricing and these will be assessed in line with the Enterprise Risk Management System (see Assignment 1).

This paper focuses on risks relating to the unit registry and is designed for use by the client-servicing department.

In practice RANDOMCORP has several unit registries for different investment vehicles, each of which has different exposures to error and different consequences of those errors.

This document consolidates the data for all unit registries into one generic entity. The purpose is to determine the approach to adopt for all unit registries in RANDOMCORP. In addition to our recommendations, further work should be done to assess and treat the risks relating to each specific database, as well as to re-evaluate the recommendations of this report over time.

CONTENTS AND RELATED DOCUMENTS

<i>Context</i>	<i>1</i>
What is the unit registry?	1
Why is this important?	1
Scope and purpose	1
<i>Contents and related documents</i>	<i>2</i>
<i>Overall Approach</i>	<i>3</i>
<i>Risk identification</i>	<i>3</i>
Workshop	3
<i>Risk analysis and evaluation</i>	<i>4</i>
Sources of Risk - The fault tree	4
Consequences of Risk - the event tree	7
Controls in place – the bow tie diagram	9
<i>Recommendations</i>	<i>10</i>
Minimising the occurrence of failure	10
IT Interfaces and processes	10
Keep focussing on Culture and training	11
continue checking new risks	11
Minimising the impact of failure that has occurred	11
Reconcile reports used to buy and sell units	11
Pay out compensation promptly	11
Legal agreements with information providers	11
Regular testing of DR and BCP	11
<i>Appendices</i>	<i>12</i>
Calculations underpinning the fault tree	12
Diagram showing where unit registries fit into unit pricing errors	13

Related documents	Referred to as
Standards Australia, HB 436 2004, <i>Risk management Guidelines: A companion to AS/NZS4360: 2004</i> , SAI Global	Risk Management Standards
- The recognised standard for managing risks in Australia.	
Notes provided by University of New South Wales for the Risk Management course GBAT 9105 as part of the Master of Business and Technology course (Semester 1, 2006)	Risk Management Course Guide
Risk management Assignment 1 – James King	Assignment 1
- The recommended Risk Management System (hypothetically) implemented across the RANDOMCORP organisation	
<i>Unit Pricing Guide to Good Practice</i> , November 2005, Jointly published by APRA and ASIC. As downloaded from www.apra.gov.au 1 May 2006.	Unit pricing guide
- A guide produced jointly by APRA and ASIC to help financial services organisations understand and comply with their obligations with respect to unit pricing.	

OVERALL APPROACH

The overall approach used in this paper is consistent with the risk management diagram in Assignment 1.

- Identify risks through a number of sources.
- Analyse the causes, outcomes and existing controls. In this case:
 - Causes were identified and communicated through a fault tree
 - Outcomes were analysed through an event tree; and
 - Existing controls and barriers to risks were communicated through a bow tie diagram.
- Recommend treatments for risks; and
- Monitored and more widely communicate both the risks and the treatments. They will also be reassessed (and improvements made) on an ongoing basis.

RISK IDENTIFICATION

WORKSHOP

Risks were identified through a workshop with stakeholders of the unit registry across RANDOMCORP.

The stakeholders who participated in the workshop were:

- A representative from the customer service help desk
- A representative from the risk management team
- A database administrator from IT
- Representatives from the internal audit team
- The unit registry team

The workshop consisted of the following phases or iterations.

1. Review the processes used in updating and reporting from the unit registry. This was based on the generic model for identifying risks, contained in section 3 of the Risk Management Course Guide:
 - a. Divide the processes associated with the unit registry into steps, based on a system flowchart prepared by a member of the unit registry team.
 - b. For each step, identify required inputs, actions and outputs.
 - i. Identify anything that can cause deviations or data errors in each input
 - ii. Identify these as risks

- iii. Identify any controls that are in place to protect from those risks
 - c. Identify outputs for each step, including any data interfaces or reports
 - i. Consider how this outputs may be prone to error
 - ii. Identify these as risks
 - iii. Identify any controls that are in place to protect from those risks
2. Review documentation prepared for the workshop for additional risks:
 - a. A list of previous incidents recorded in the Enterprise Risk Management database, presented by the risk management team representative.
 - b. Errors coming out of reconciliations conducted on investment trusts, presented by one of the finance team.
 - c. A summary of any findings and recommendations in previous audits (both internal and external), presented by the internal audit representative.
 - d. A summary of incidents that were raised with the customer service helpdesk, presented by a representative of the help desk.
3. The workshop then brainstormed any other causes that could potentially lead to the unit registry not providing the correct data.
4. These risks were then further analysed as described below.

RISK ANALYSIS AND EVALUATION

SOURCES OF RISK - THE FAULT TREE

A fault tree is a tool used to investigate and communicate the possible events (“faults”) that can lead to an outcome (the “head event”). Although generally used to review negative outcomes the same approach can be used to identify opportunities or desired goals.

When used to explore an event that has already occurred, fault trees start with the problem and then seek to find the most probable sequence of events that led to that problem occurring.

When looking forward, we start with the event we are analysing and then review the causes that might lead to that event. We then review these in turn to see what could cause them, and to understand the underlying likelihood. In line with this our approach was to:

1. Start with the risk we are analysing - “unit registry does not provide correct data”. This is then called the “head event”.
2. Determine all the events which could immediately cause the head event. These are called causal events.
3. Determine the relationships between these causal events and the head event.
 - a. Where any combination of one or more of the causal events can cause the head event, add an “or” gate.

Figure 1 - Unit registry fault tree (events leading to failure)

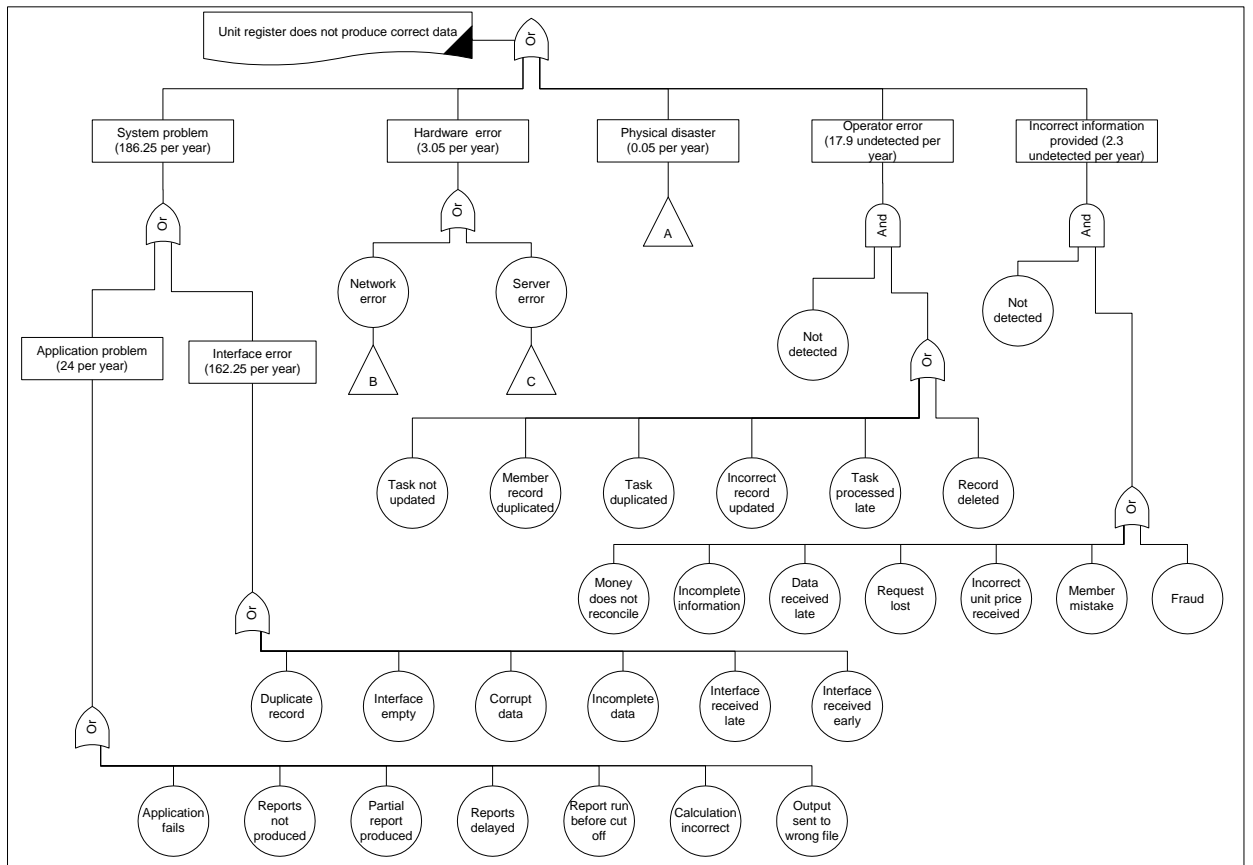
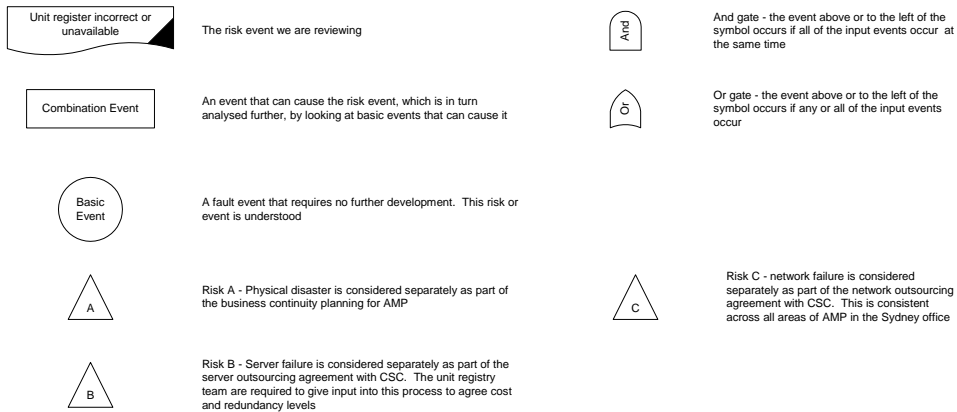


Figure 2 - key to symbols used in the fault tree



Number of occurrences per year

Based on previous data, the company can expect to receive 210 instances of the unit registry failing to provide the correct data each year.

- By far the greatest cause is system problems (primarily interface errors). This suggests that further work should be done in investigating these areas for improvement.
- The greatest number of errors is “incorrect information recorded” (557 occurrences per year). But these were rarely entered into the system without detection (the and gate). Consequently we expect that our existing controls in this area are already strong and need to be maintained. This also suggests that we have a good culture around quality among the customer service team.

However it is impossible to know whether any of these numbers are significant without knowing what the likely consequence of failure is.

CONSEQUENCES OF RISK - THE EVENT TREE

After identifying the sources of risks, a further workshop was held to identify the outcomes that could result from each event identified as a risk. This was done using an event tree.

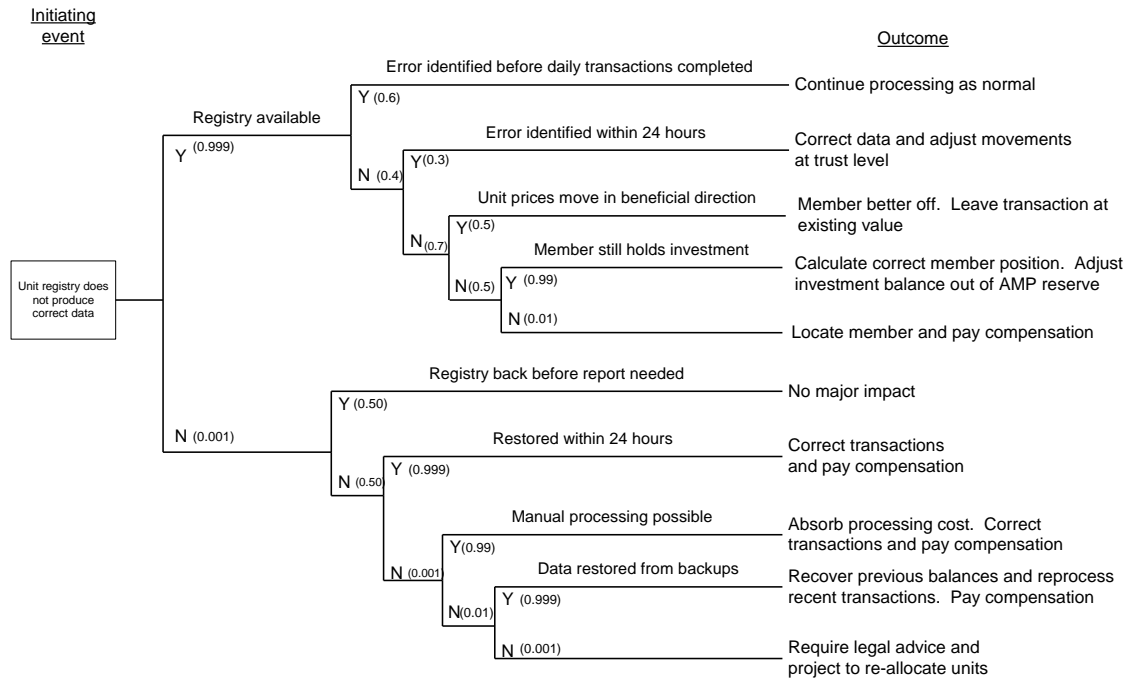
Where a fault tree is used to map back what causes can LEAD TO a particular event, an event tree maps the possible scenarios and outcomes that can be caused BY the particular event. These outcomes can be either beneficial or detrimental.

The process followed here was:

1. Assume that the initiating event (not providing correct data) has occurred and work out could immediately happen as a result. Each different result is then listed as a scenario.
 - a. Turn these scenarios into Boolean (yes/no) questions to allow the calculation of probabilities for each outcome.
 - b. To calculate the probability of the statement being true, assess what percentage of the time the statement will be true if the preceding statement was true.
2. For each scenario:
 - a. If the scenario itself can meaningfully lead to a number different of outcomes or scenarios, then repeat step 1, with the new scenario being treated as the initiating event and each new outcome as a scenario.
 - b. Otherwise record the scenario and list the resulting outcome (consequence) that will be incurred.
 - i. For the purpose of the RANDOMCORP Enterprise Risk Management System, classify the impact as a financial impact in line with the categories included in the consequence table provided in that system.
 - ii. Where appropriate also consider the corporate reputation impacts listed in the same table.
3. To assess the total likely impact of the unit registry failing to provide the correct data:

- a. Multiply the probabilities of each statement being true, by the probability of the previous statement being true.
- b. Multiply the cumulative probability of the final scenario being true by the estimated impact of that scenario.
- c. Add these amounts together to give a total expected impact.

Figure 3 - Event tree for unit registry not producing correct data



Probability and impact of each outcome

Outcome	Calculation	Probability	Likely cost (\$)	Predicted impact (\$)
Continue processing as normal	0.999×0.6	0.5994	2,000	1,199
Correct data and adjust movements at trust level	$0.999 \times 0.4 \times 0.3$	0.1199	10,000	1,199
Member better off. Leave transaction at existing value	$0.999 \times 0.4 \times 0.7 \times 0.5$	0.1399	0	0
Calculate correct member position. Adjust investment balance out of RANDOMCORP reserve	$0.999 \times 0.4 \times 0.7 \times 0.5 \times 0.99$	0.1385	15,000	2,077
Locate member and pay compensation	$0.999 \times 0.4 \times 0.7 \times 0.5 \times 0.01$	0.0014	20,000	28
No major impact	0.001×0.5	0.0005	0	0

Outcome	Calculation	Probability	Likely cost (\$)	Predicted impact (\$)
Correct transactions and pay compensation	0.001*0.5*0.999	0.0005	100,000	500
Absorb processing cost. Correct transactions and pay compensation	0.001*0.5 *0.001*0.99	0.0000	10m	5
Recover balances and reprocess recent transactions. Pay compensation	0.001*0.5*0.001 * 0.01 * 0.999	0.0000	50m	25
Require legal advice and project to re-allocate units	0.001*0.5*0.001 * 0.01 * 0.999	0.0000	100m	0
Total potential impact		1.0	-	5,007

Thus RANDOMCORP should expect to lose \$5,007 each time the failure occurs. If the failure occurs an expected 210 times during the year, then the annual expected cost of this failure is around \$1m.

The outcomes expected to cost RANDOMCORP the most each year are errors in data leading to members receiving the wrong number of units. Thus RANDOMCORP should concentrate on controls to protect from these outcomes.

In addition, however, there are 3 outcomes that could cost RANDOMCORP \$10m or more (as well as significant brand damage). The level of the potential impact means that these outcomes need to be considered carefully even if there is only a slim chance of them occurring.

CONTROLS IN PLACE – THE BOW TIE DIAGRAM

Having considered the causes of the risk to occur and the potential consequences of the risk, we then considered the controls that act as barriers to protect RANDOMCORP from the risk eventuating, or that aid recovery in treating the risk.

These were taken from the initial workshop that looked at the processes involved and were then added to in a further brainstorming session. The major findings are that

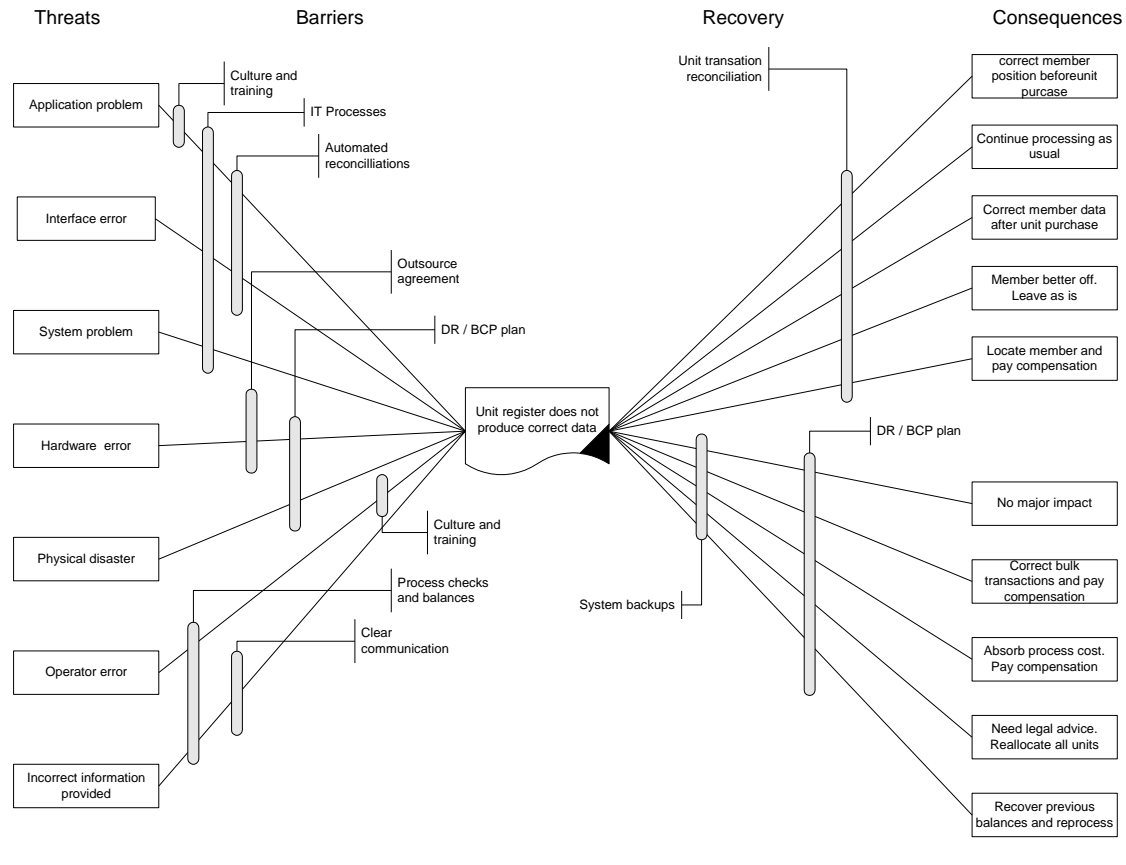
- There are strong controls in place with respect to disaster recovery and business continuity, which protect us from the impact of registry not being available.
- The customer service team detects almost all customer information errors.
- The controls around IT interfaces and automatic updates, as well as the way IT changes are made, have some minor gaps and should be further reviewed.

The results are summarised in a bow tie diagram (below). This is a simplified picture of

- The causes (called threats) that can lead to the unit registry failing to provide the correct information (called the failure event);
- The controls (called barriers) in place to stop threats from leading to the failure event;

- The controls (called recovery) in place to mitigate the damage (or stop the benefit) caused if the failure event does occur; and
- The outcomes (Consequences) of the failure event.

Figure 4 - Bow tie diagram



RECOMMENDATIONS

MINIMISING THE OCCURANCE OF FAILURE

IT INTERFACES AND PROCESSES

IT interfaces are the leading cause for failure, while system failure has the potential to create the worst outcomes (complete process failure).

We therefore recommend a separate project be initiated to investigate these causes in far greater detail. The scope of the project should include both hardware, software and process issues.

Ensuring System reliability as part of business cases

Anecdotal evidence suggests that many of the system errors are caused by system complexity and the pressure to add new functionality quickly in line with business strategy.

While objective evidence will not exist until the analysis is performed, we believe that an interim step should be to ensure the issue is not further exacerbated. To this end we have spoken to the project office to have the business case template update to include

- A compulsory requirement to analyse and maintain system reliability for any changes impacting unit registries.
- Building or updating a reconciliation process for any interfaces before they are implemented or upgraded.

KEEP FOCUSING ON CULTURE AND TRAINING

As discussed in the RANDOMCORP Enterprise Risk Management System, a risk management culture is critical to managing all risks in the company. Our analysis suggests strong controls around the accuracy of data, but a potential for significant impacts if this fails.

We recommend continued focus on staff training around:

- The importance of risk management;
- The accountabilities and expectations of their roles; and
- The appropriate skills and processes involved in their roles.

CONTINUE CHECKING NEW RISKS

This study is conducted at a point in time and considered all unit registries as one entity.

In fact they are several individual systems and therefore further analysis should be conducted with respect to each system to build on the findings in this report.

In addition, in line with the Enterprise Risk Management System, the risks identified in this document should be reviewed annually, or more frequently if circumstances change.

MINIMISING THE IMPACT OF FAILURE THAT HAS OCCURRED

RECONCILE REPORTS USED TO BUY AND SELL UNITS

Currently, when reports are produced and units are purchased, the unit registry processes end. However our analysis shows that considerable savings are made when any errors are found in the first 24 hours of unit purchases.

We recommend building in an automated reconciliation process to pick up some of the errors. Also, to investigate possible processes that will detect data irregularities or other errors.

PAY OUT COMPENSATION PROMPTLY

The cost of errors increases over time. Therefore prompt correction is financially beneficial to RANDOMCORP as well as beneficial to the brand. We recommend a focus in process and resourcing to ensure any detected errors are promptly dealt with.

LEGAL AGREEMENTS WITH INFORMATION PROVIDERS

Where information is received from other financial institutions and this information can lead to errors in our data. We cannot abdicate our role in checking this data, but we can receive some protection through sound contracts.

REGULAR TESTING OF DR AND BCP

We currently conduct regular tests of our systems and business continuity processes. We recommend these tests include some specific scenarios around restoration of unit registries.

APPENDICES

CALCULATIONS UNDERPINNING THE FAULT TREE

	Frequency for base events (occurrence per year)	Cumulative frequency	Probability for And gate	Total
Application fails	1			
Reports not produced	6			
Partial report produced	3			
Reports delayed	7			
Report run before cut off	4			
Calculation incorrect	2			
Output sent to wrong file	1			
Application problem		24		
Duplicate record	88			
Interface empty	4			
Corrupt data	0.25			
Incomplete data	56			
Interface received late	12			
Interface received early	2			
Interface error		162.25		
System problem				186.25
Network error	3			
Server error	0.05			
Hardware error		3.05		3.05
Physical disaster				0.05
Task processed late	95			
Task not updated	86			
Member record duplicated	25			
Task duplicated	12			
Incorrect record updated	17			
Record deleted	1			
Operator error (note that quality reports show 92.4% of errors are detected and corrected)		236	0.076	17.9
Money does not reconcile	16			
Information incomplete	225			
Data received late	35			
Request lost	3			
Incorrect unit price rec'd	2			
Member mistake	264			
Fraud	12			
Incorrect information (note that quality reports show that 99.6% of errors are detected and corrected)		557	0.004	2.3
Total failures per year				209.55

DIAGRAM SHOWING WHERE UNIT REGISTRIES FIT INTO UNIT PRICING ERRORS

Figure 5 - taken from the Unit Pricing Good Practice Guide. Copyright Australian Prudential Authority and Australian Securities and Investments Commission. Reproduced with permission

Figure 2: Key elements of the unit pricing cycle

