Summary of Business Case Review for the Invitation to Provide Commercial Opportunities

15 September 2009

Table of Contents

1 Introduction

1 This document is a summary of the igovt Business Case review prepared in May 2009; it has been produced to be provided to organisations who have expressed an interest in responding to the Invitation to Provide Commercial Opportunities[1] conducted in September 2009.

2 Purpose of the Review

2 The business case review provided an analysis of the five original authentication programme business cases and consolidates the drivers, objectives, benefits and key themes from those documents into this review.

3 The review updates original parameters and assumptions where necessary in order to provide a 10-year forward estimate of the programme's benefit streams, further supported by a quantitative risk analysis.

3 Scope and Approach

3.1.1 Scope

4 The analysis adheres to the scope and intent of the original business cases without introducing new major themes or items of scope that were not clearly signalled in the original business cases.

5 For example commercial sector involvement may significantly alter the scope and nature of some of the benefit streams analysed in this document. For the purposes of this analysis no consideration of the impact of such involvement has been made.

6 The analysis is limited to costs and benefits from a whole of government perspective and does not consider funding mechanisms.

3.1.2 Approach

7 The approach included:

(a) Review of the original business case documents

(b) Investment Logic Mapping completed from a "green fields" perspective, with the involvement of key stakeholders from a number of large agencies

(c) Update of the benefit calculations to reflect an improved understanding of how benefit streams are likely to arise over time

(d) Performing a quantitative risk analysis (QRA) on the core variables that drive the calculation of the benefit streams.

8 Note that the igovt logon service (formerly known as GLS) and the identity verification service (IVS) are clearly inter-related in terms of uptake. However, attempting to leverage their inter-relationships has a tendency to obscure clear analysis. Therefore, with respect to logon service the review assumes that the identity verification service is not there.

[1] Refer http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Identity-Verification-Service-Online-identity-services-commercial-relationships?OpenDocument

9 With respect to the identity verification service the review makes no assumption about the positive influence that the logon service will have on increased adoption of online services.

10 A moderately conservative approach has been taken in recalculating benefit streams throughout the review exercise.

4 Executive Summary

4.1 Drivers

11 The authentication programme is founded on an assumption that the Internet will become a mission critical channel for the delivery of a range of frontline services for government.

12 The Internet is becoming an integral part of people's daily lives and they are conducting an increasing amount of their day-to-day affairs online.

(a) 78% of New Zealanders over the age of 15 use the Internet, and 55% of them describe the Internet as either important or very important in their daily lives (AUT World Internet Project).

(b) People expect to be able to do business with government just as easily as they can with other organisations, such as banks and airlines.

13 The current situation of each agency establishing their own relationship with their own customer base is unsustainable.

(a) Costs are duplicated and a frustrating compliance burden is created with a growing number of user interfaces and logon solutions.

(b) Potential reduction of the range of online services that can be offered due to an incomplete solution that lacks the fundamental ability to verify their identity at the point where people enter into an online relationship with government.

(c) A reduction in the motivation of the public to use online services if parts of the transaction must still be completed through other channels.

(d) Reduction in uptake of online services due to a lack of trust in the use and treatment of identity information online.

14 The overall impact will be delayed access to online service-delivery models both for individuals and government.

15 The lack of consistent and integrated identity process in relation to the use of the online channel will increase the risk of identity related crime.

4.2 Benefits

16 The programme's benefit streams were summarised in the Investment Logic Mapping exercise as follows:

(a) Reduced cost to government of implementing and running on-line services requiring identity,

(b) Improved user experience with online government services,

(c) Reduced government agency transaction costs for services requiring identity, and

(d) Reduction in incidence and impact of identity crime.

17 A single logon for the whole of government means an efficient and familiar logon experience, both for people, and for agencies. It:

(a) creates significant tangible benefits by reducing un-necessary duplicate costs,

(b) increases security by enabling more of it to be efficiently managed in one place, and

(c) makes it easier for people to deal with government online.

18 In year ten of its operation GLS will result in a single online community in excess of 1.6m users transacting on a regular basis across government.

19 Technology makes it possible to "reuse" a high-strength identity verification event, such as obtaining a passport, repeatedly and at significantly lower cost than would otherwise be incurred in establishing that a person is who they claim to be.

20 The availability of a real-time and cost efficient method of establishing confidence in a person's identity will create new opportunities for using such a service that have not currently been considered.

21 A single large body of online relationships gives rise to new ways of doing business and increased value for both the users of those services and the delivery organisations involved e.g Trademe.

22 GLS aggregates the value of government's online relationships with individuals and IVS aggregates the value of identity verification across government. Through that aggregated value it is possible to deliver new services of increasing value to individuals and government, whilst also deriving significant tangible benefits.

23 igovt provides a government-wide identity infrastructure that is user-centric and privacy protective, without which that aggregated value cannot be accessed and delivered for all agencies to use equally.

24 igovt is a key piece of infrastructure that make new business models possible, and they drive value out of existing investments by ensuring that people have a good and efficient experience when interacting with government services online.

25 GLS will improve a person's ability to engage with the government online and in doing so is likely to gradually improve uptake of those services. IVS in turn has a significant impact on government's ability to deploy *complete* services online, which will increase the range of services requiring authentication by GLS.

4.3 Summary of Financial Analysis

4.3.1 igovt logon service (GLS)

26 The QRA found that there is a ten-year tangible benefit range from July 2009 of between $321m and $727m between the 10th and 90th percentiles for likelihood, with the mean value at $514m.

27 Programme costs over the ten year period are estimated to be $65m.

28 The GLS benefit streams are divided into three main areas (the IVS is also divided into the same three areas):

(a) Displaced duplicate costs for the crown

(b) Trust and Confidence in the online channel, the cost of maintaining such trust and confidence being more efficient for the crown using GLS than without GLS

(c) Efficient user experience for the public.

29 GLS costs have been revised in order to defer any expenditure that is not immediately necessary with a view to ensuring that GLS benefit streams are achieved at a meaningful level (benefits exceeding yearly costs) as quickly as is feasible. This means taking a demand based view of any further functional enhancements and fully realising and utilising the benefits of scale following the Government Technology Services group's move from the State Services Commission to the Department of Internal Affairs.

30 The summary position for GLS following the review is that:

(a) The cumulative net benefit position for GLS will be positive by Year 4.

(b) The yearly net benefit position for GLS will be positive by Year 3.

(c) The ten year net benefit is $313m

(d) The ten year NPV is $160m

31 The key risk to the GLS benefit streams is achieving volume in its user base, and integrating a number of medium to large size agencies quite quickly.

32 The basic delivery risk in relation to GLS is regarded as low. GLS has a history of successful delivery and by June 09 will have integrated twelve agencies successfully with an increasingly reducing cost of integration.

33 In summary GLS will soon achieve good levels of uptake and costs have been scaled back to defer expenditure over the next three years until benefit streams exceed costs.

4.3.2 igovt identity verification service (IVS)

34 The QRA found that there is a ten-year tangible benefit range from July 2009 of between $320m and $646m between the 10th and 90th percentiles for likelihood, with the mean value at $472m.

35 Programme costs over the ten year period are estimated to be $57m.

36 The summary position for IVS following the review is that:

(a) The cumulative net benefit position for IVS will be positive by Year 5.

(b) The yearly net benefit position for IVS will be positive by Year 4.

(c) The ten year net benefit is $309m

(d) The ten year NPV is $154.8m

37 The key risk for IVS is again achieving uptake:

(a) IVS must achieve membership volumes, which the programme considers can only be achieved efficiently through a “co-apply” model.

(b) IVS members must also be able to use IVS to verify their identity online.

(c) IVS needs to be achieved through an integrated plan amongst a number of collaborating agencies that balances increasing IVS membership with suitable availability of services allowing for its use.

(d) IVS is currently proposed as a service that will operate at “high strength”, allowing a high strength transfer of a high strength identity from one agency (DIA) to many others as required.

(e) IVS uptake can be achieved at lower risk by adopting a blended model that allows for IVS membership and use at medium strength in the early years.

(f) Gradually upgrading IVS through a medium strength phase to a higher strength phase also means that there is an opportunity to plug-in a larger number of medium strength identity sources.

38 In summary the IVS benefit streams remain significant, but achieving uptake in order to establish those benefit streams will be most effectively achieved through integrated planning amongst a number of collaborating agencies.

4.4 Consequence of Not Proceeding

4.4.1 igovt logon service (GLS)

39 Without GLS:

(a) Agencies will still need to offer logon capabilities to allow people to access services requiring authentication.

(b) Smaller agencies will find it hard to afford stronger forms of authentication and as a consequence will

(i) either refrain from offering services of higher value/risk, or

(ii) will use weaker forms of authentication and offer those services at higher risk.

(c) Individuals will use an increasing number of usernames and passwords to access government services.

(i) They are likely to adopt weak password practices as a result, and also much more likely to forget those passwords and usernames on a regular basis, which will result in a number of calls to call centres.

(ii) This increasing number of usernames and passwords will also act as a disincentive to use the online channel.

(d) It is likely that logon security will, on average, be weaker than it will be in the case of GLS.

(e) At some point it's likely that individuals will be issued more than one 2-factor logon devices by different agencies.

(f) The opportunity to develop a single integrated online community interacting regularly with government through a point of "high trust" will be lost, and future benefit streams made possible through the ability to interact with and deliver new services to this community will be foregone.

(g) The ability to deliver other identity related services on top of the igovt platform will be lost.

4.4.2 igovt identity verification service (IVS)

40 Currently checking identity at source as described in the Evidence of Identity (EOI) Standard is hard to do for most agencies outside of DIA and the common approach is to resort to the matching of batch data.

41 Most agencies need to verify identity for the purposes of their first interaction with a person and then thereafter confirm that it's the same person they previously dealt with.

However to get the level of confidence required, they are faced with having to carry out the same expensive establishment process each time. This leads either to expensive processes, or to inadequate but less expensive identity verification processes because of the current lack of availability of appropriate (online) verification services from DIA.

42 This situation will continue until identity services offered by DIA, in particular IVS and the Data Validation Service (DVS) are commonly adopted amongst agencies.

5 Financial Summary

Summary (millions)		**GLS**	**IVS**
	Ten year Benefits	**379m**	**367m**
	Ten year Costs	**65.6m**	**57.4m**
	Ten year Net Benefit	**313.4m**	**309.7m**
	Ten year NPV	**160m**	**154.8m**
	Year in which benefits exceed costs	**Year 3**	**Year 4**
	Year in which cumulative benefits exceed cumulative costs	**Year 4**	**Year 5**
Tangible Benefit Streams			**Value**
GLS	**Duplicate Cost Avoidance**		
	Reduction in customer support costs		177.7
	Re-use of stronger credentials amongst agencies		125.7
	Avoidance of duplicated infrastructure		19.8
	Avoided call-centre costs		1.9
	Efficient access to online services		
	Reduced key-management costs		40.7
	Trust and Confidence in the online Channel		
	Centralised security assessments and audits		8.9
	Centralised major security upgrades		4.4
	Centralised management of break-in attempts		1.0
	Total		**379m**
IVS	Displacing identity verification costs		238.5
	Saving people time when proving who they are		65.8
	Reduction in identity crime/fraud		62.8
	Total		**367.1m**
Other Benefits and Added Value			
	Establishing a framework for further re-use of government data		
	Single integrated online community and online identity infrastructure for government		
	International Leadership		
	Improved Security		

43 Notes:

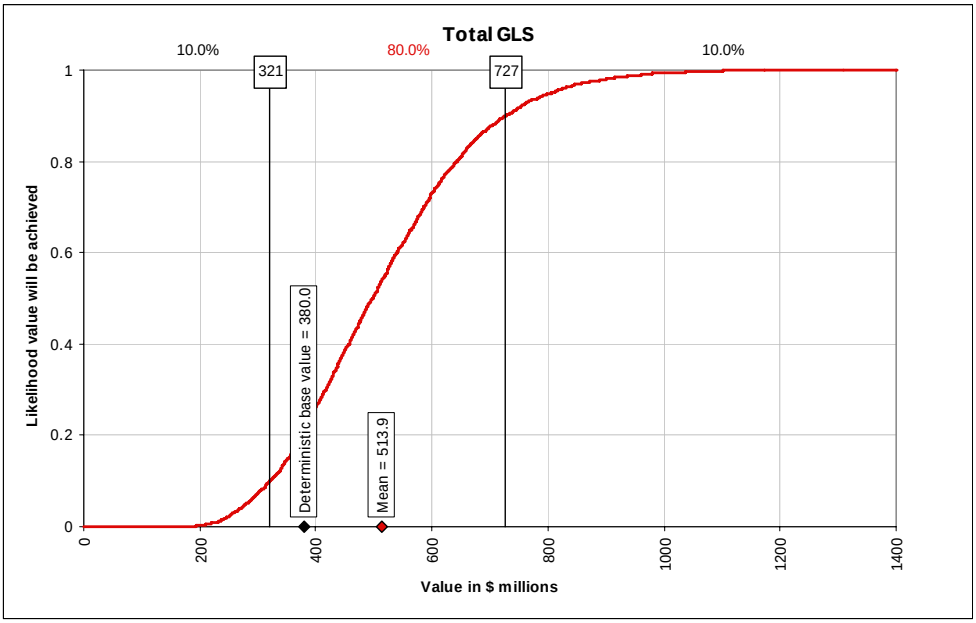
(a) The benefit figures and NPV figures shown in the table above are taken from the benefit calculations that fed into the QRA exercise. This places them at approximately the 20th percentile for likelihood. This has been done because the QRA exercise does not yield individual yearly benefit figures, but only an overall summary figure. See the next section, in which the "deterministic" values equate to the figures in the above table.

(b) Some allowance will need to be made for the phasing of recoverable costs, such as call centre costs, which are passed on to agencies. These are typically incurred by GLS before they can be recovered from agencies creating a small period of time where GLS must carry those costs.

6 Quantitative Risk Analysis

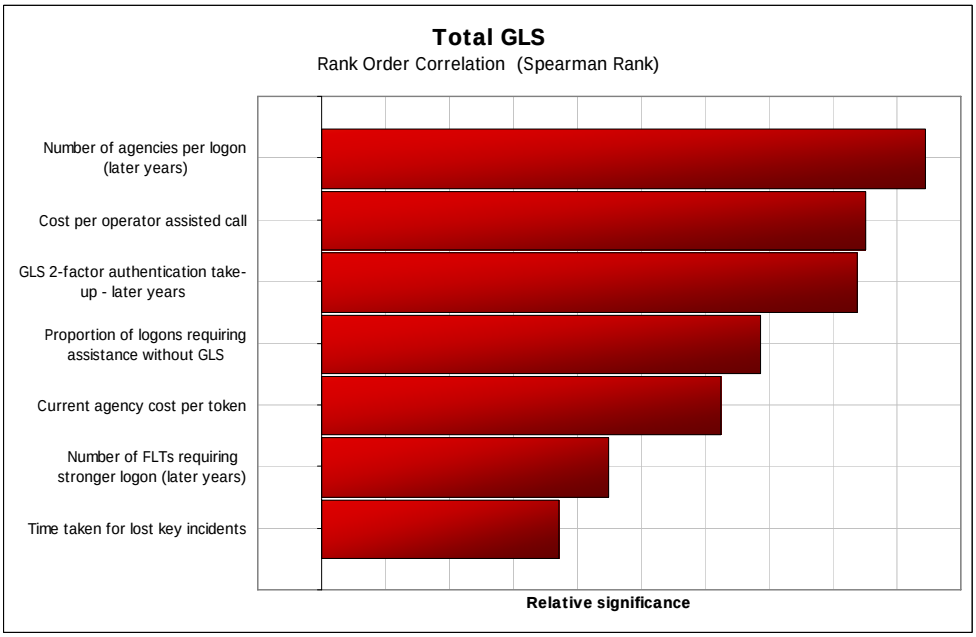
44 A quantitative risk analysis was performed using an external facilitator. The results are presented below:

6.1 igovt logon service (GLS)



45 The chart shows the result of the QRA simulation for GLS. It shows that there is a benefit range of between $321m and $727m between the 10th percentiles, with the deterministic value sitting on approximately the 20th percentile, and the mean value at $513.9m. The deterministic value is the value originally present in the underpinning spreadsheet that fed into the QRA.

46 The following chart shows the relative importance of the key variables as shown by the simulation. The chart doesn't show all variables used in the QRA, only key variables.

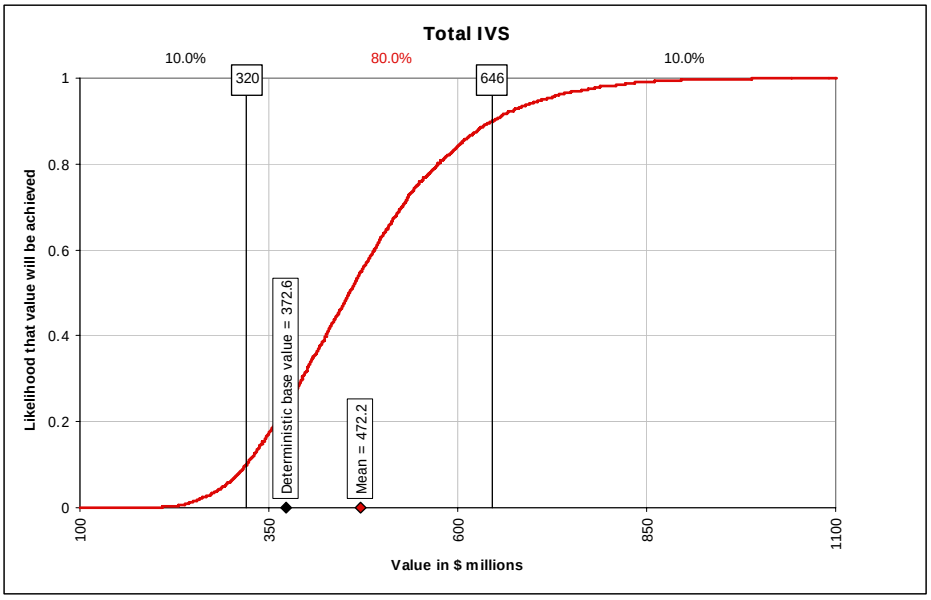


47 The chart shows that the number of agencies per logon (the degree of re-use of a GLS logon at across more than one service) is the key variable.

48 This variable ranges from a value of 1.3 in June 2010 through to a value of 5.8 in 2018. This variable drives both the reduction in customer support costs benefit, and the user-experience benefits. The variable also reflects the founding assumption that the Internet will become a mission critical channel for government.

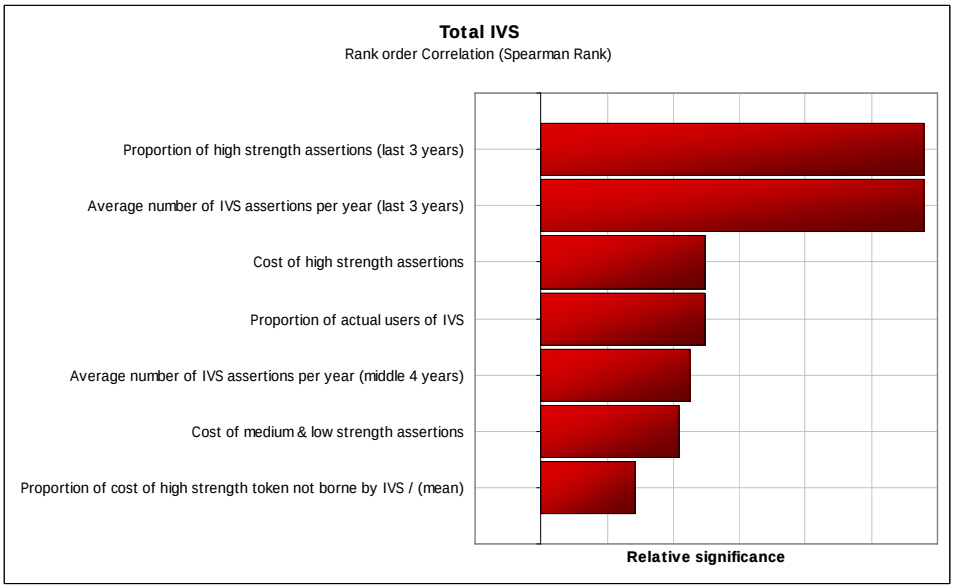
49 However, the importance of this variable is such that it will require careful monitoring to assess its ongoing behaviour as larger communities of users come on board during 09/10 and 10/11.

6.2 igovt identity verification service (IVS)



50 The chart shows the result of the QRA simulation for IVS. It shows that there is a benefit range of between $320m and $646m between the 10th percentiles, with the deterministic value sitting on approximately the 27th percentile, and the mean value at $472m.

51 The following chart shows the relative importance of the key variables as shown by the simulation:



52 The chart shows that the proportion of high strength assertions in the last three years of the business case, and the average number of IVS assertions per year in the last three years, are the dominant variables.

53 The new business case calculations for IVS have "phased" the introduction of high strength assertions over three periods — years 1–3 having none as the services is established through the use of medium strength, years 4–7 having 10% of assertions made at high strength, and years 8–10 having 20% of assertions made at high strength.

7 Other Benefits

54 This section details other benefit streams identified during the review that are not given monetary values in the financial summary.

7.1 General

55 igovt will help to preserve trust and confidence by giving people a common entry point into government that is familiar and efficient.

7.2 Framework for further re-use of government data

56 igovt establishes a framework that can be readily applied to the further re-use of government data in a privacy protective manner. Any personal information that has already been established with government by an individual can be re-used in a similar manner to that adopted by IVS.

7.3 Single integrated online community

57 igovt creates a point of "high trust" through which a single integrated online community will interact with government, which is projected to include the majority of New Zealanders by year 10 of this review (2018).

58 The value of that community, both to government and to individuals, is significant as it will make new operational models and future benefit streams possible.

7.4 International Leadership

59 The authentication programme is currently engaged in a number of discussions regarding reuse of the programmes capability and services in other jurisdictions.

60 The programme is in the early stages of engagement with the World Bank to consider how the programme's services might be used in a number of countries.

61 The release of a suite of authentication and identity verification standards for igovt in 2006 has seen the standards attract wide domestic and international praise, to the point where the New Zealand government is now a leading international player. This means that New Zealand's focus on practical, privacy- and citizen-centric solutions is now being adopted in global standards, which will greatly reduce the cost in outyears of modifying inbound vendor software.

7.5 Improved Security

62 igovt uses relevant standards and best practice in relation to identity and authentication, and is delivered through a secure and reliable infrastructure that undergoes regular review and audit, both internally and externally, including active penetration testing.

7.6 Online identity infrastructure

63 IVS, and related services such as the Data Validation Service (DVS), will create a consistent and integrated suite of identity services that reduce the incidence of weak or broken linkages between various agencies.

64 There may be some potential for use of the programme's services in relation to anti-money laundering legislation / countering terrorism finance.

65 IVS has obvious relevance for the banks in reducing fraud through confidence in identity, and represents an online equivalent to the practices they currently adopt in using New Zealand identity documents to check the identity of transacting parties.

66 IVS has a significant beneficial effect on information quality and data cleansing issues which have not been factored into any benefit stream.

67 IVS will also, over time, deliver the ability to keep identity data up-to-date (under the consent and control of the individual) in a low cost manner.

7.7 Commercial Sector Involvement

68 There is significant potential of commercial sector involvement in terms of the potential impact on benefit streams. If we assume that 35% of GDP is related to government services, then we can crudely extrapolate an estimate that commercial sector access to the programme's services, if available, will create approximately $1.4billion of benefits in a similar time frame.

69 These benefits will arise in a similar manner, through reduced investment required by companies, cost effective channel management options that are better supported, reduction in identity-related fraud and improved outcomes for customers with even greater utilisation of the same credentials.

70 Benefits might occur through, for example:

(a) The ability to open a bank account online

(b) The ability to register for Internet banking online

(c) The ability to introduce trust in identity into online transactions of any kind

(d) The ability to deliver authentication services to any business requiring it through GLS

(e) The ability for people to authoritatively re-use information about themselves, as held by government, in a commercial context (the generalisation of IVS).

(f) The ability for people to authoritatively re-use information about themselves, as held by the commercial sector, in a government context

71 Commercial sector involvement would further increase the scale and transactional density of the community of users, resulting in a service receiving very high volumes of traffic.

8 Uptake Projections / Market Size

72 This analysis has set an uptake profile for GLS that reaches 1.6m unique users by year 10.

73 The IVS uptake estimates are based on the number of people joining IVS, and the rate at which those individuals use IVS to carry out identity verification transactions within government. The review considered the following:

(a) An assessment of various life events suggests that over a ten year period people will have to verify their identity approximately once yearly. Appendix 1 provides some further insight into the known profile of identity verification events with government.

(b) Identity verification appears to have some natural clusters centred on life events such as: leaving school, entering tertiary study, entering the workplace; interaction with the benefits system; immigration; leaving the workforce.

74 These considerations, coupled with the basic uptake estimates for joining IVS, produce a transaction base that is similar to that proposed in the original business case.

75 This review has excluded the population of IVS online users from the GLS uptake figure in order to view the two sets of benefit streams somewhat independently. If included, GLS would show significantly more growth.

76 On a similar note, the figure for IVS identity assertions does not include original identity verification events that enable a person to join IVS, although it will include renewal processes that can be supported by IVS (for example applying for a passport renewal online).

Appendix 1 – Life events requiring identity – ten year averages

77 This appendix presents a high level analysis to support consideration of the likely volume of yearly identity verification events taking place within government which IVS may support.

78 A high level analysis of various life events creates a reliable "base case" for the lower bound of identity verification events that an individual is involved in, on average, over a ten year period.

Event	Frequency	Ten year avg.
Applying for/renewing a passport	Once every five years	0.2
Applying for/renewing driving licence	Once every ten years	0.1
Buying or Selling a car	Once every five years	0.2
Entering new employment	Once every ten years	0.1
Buying or Selling a house	Once every ten years	0.1
Change of address / electoral role	Once every five years	0.2
Joining any online government service	?	?

79 The following examples were also identified to show the extent of identity information used and managed by the public sector:

Transaction group	Datum	Year
Number of births and permanent or long-term arrivals to New Zealand resulting in new residents.	136,000	2005/6
Issued passports	~400,000	2008/9
Issued birth, death, marriage and civil union certificates/printouts	228,874	2005/6
Grants of citizenship to foreign nationals	27,780	2005/6
Criminal history checks (increasingly normal for employment filter)	~100,000	2007/8
Driving licenses issued	565,000	2005/6
Temporary permits to visit, study, or work, in New Zealand	~1,500,000	2005/6
Permanent Residence approvals	51,236	2005/6
IRD numbers issued	286,767	2008
Applications for income support (MSD)	675,283	2005/6
Student Allowance/Loan applications	62,193	2005/6
Community service cards issued (in circulation?)	359,334	2005/6

Appendix 2 - Glossary

Term	Meaning
2-factor	Generally refers to stronger forms of authentication over and above username and password. The origin of the name is that where username and password is a single factor (something you know) it can be made stronger by introducing a second factor – typically something you have, which is normally a physical device that can be used to provide evidence to the authenticating service that the individual attempting to authenticate is also in possession of said device.
DVS	Data Validation Service. An authenticated online service that allows agencies to check that the key identity attributes, such as that found on passports, birth certificates and citizenship documents, are consistent with source data.
EOI	Evidence of Identity – the process by which an organisation satisfies themselves that a person is who they claim to be.
Quantitative Risk Analysis	A process of assessing the probabilistic ranges of a number of variables and simulating the overall impact of a set of scenarios driven by these probabilities on the overall range of benefit streams arising. This process can also be executed for costs, but that has not been done for this analysis. The programme has a history of sound cost estimation and, on average, almost nil use of contingency.