ACT Government
Chief Minister, Treasury and Economic Development

Freedom of Information Publication Coversheet

The following information is provided pursuant to section 28 of the *Freedom of Information Act 2016*.

FOI Reference: CMTEDDFOI 2020-219

Information to be published	Status
1. Access application	Published
2. Decision notice	Published
3. Documents and schedule	Published
4. Additional information identified	No
5. Fees	Waived
6. Processing time (in working days)	20
7. Decision made by Ombudsman	N/A
8. Additional information identified by Ombudsman	N/A
9. Decision made by ACAT	N/A
10. Additional information identified by ACAT	N/A

From: [redacted]
To: CMTEDD FOI
Subject: Freedom of Information request
Date: Wednesday, 18 November 2020 12:07:09 PM

Please find online enquiry details below. Please ensure this enquiry is responded to within fourteen working days.

Your details

All fields are optional, however an email address OR full postal address must be provided for us to process your request. An email address and telephone contact number will assist us to contact you quickly if we need to discuss your request.

Title: [redacted]
First Name:
Last Name:
Business/Organisation:
Address:
Suburb:
Postcode:
State/Territory:
Phone/mobile:
Email address:

Request for information

(Please provide as much detail as possible, for example subject matter and relevant dates, and also provide details of documents that you are not interested in.)

Under the Freedom of Information Act 2016 I want to access the following document/s (*required field):	ACT Government acquired Salesforce platform for it's ACT digital account services by the Office of the Chief Digital Officer. Please provide any documentary evidence such as the Business Case, the Procurement Plan Minute, the Tender Evaluation Report or the approval of the Tender Evaluation Report or others that demonstrates an open tender process had been exercised. If it wasn't an open tender, please provide any documents that justify the reason why the open tender wasn't an option.
I do not want to access the following documents in relation to my request::	Any personal information or confidential texts can be masked or deleted from the documents.

Thank you.
Freedom of Information Coordinator

ACT Government
Chief Minister, Treasury and Economic Development

Our ref: CMTEDDFOI 2020-219

[redacted]

via email: [redacted]

Dear [redacted]

FREEDOM OF INFORMATION REQUEST

I refer to your application under section 30 of the *Freedom of Information Act 2016* (the Act), received by the Chief Minister, Treasury and Economic Development Directorate (CMTEDD) on 18 November 2020.

Specifically, you are seeking: "*ACT Government acquired Salesforce platform for its ACT digital account services by the Office of the Chief Digital Officer. Please provide any documentary evidence such as the Business Case, the Procurement Plan Minute, the Tender Evaluation Report or the approval of the Tender Evaluation Report or others that demonstrates an open tender process had been exercised. If it wasn't an open tender, please provide any documents that justify the reason why the open tender wasn't an option.*"

Authority

As an appointed Information Officer under section 18 of the Act, I am authorised to make a decision on access or amendment to government information in the possession or control of CMTEDD.

Timeframes

In accordance with section 40 of the Act, CMTEDD is required to provide a decision on your access application by 16 December 2020.

Decision on access

Searches were completed for relevant documents and 20 documents were identified that fall within the scope of your request.

I have included as **Attachment A** to this decision the schedule of relevant documents. This provides a description of each document that falls within the scope of your request and the access decision for each of those documents.

I have decided to grant access in full to eight documents and partial access to five documents relevant to your request. I have decided to refuse access to seven documents as I consider them to be:

- contrary to the public interest information under schedule 1; or
- information that would, on balance, be contrary to the public interest to disclose under the test set out in section 17 of the Act.

My access decisions are detailed further in the following statement of reasons and the documents released to you are provided as **Attachment B** to this letter.

In accordance with section 54(2) of the Act a statement of reasons outlining my decisions is below.

Statement of Reasons

In reaching my access decisions, I have taken the following into account:

- the Act;
- the content of the documents that fall within the scope of your request.

Exemption claimed

My reasons for deciding not to grant access to the identified documents and components of these documents are as follows:

<u>Information that would, on balance, be contrary to the public interest to disclose under the test set out in section 17 of the Act</u>

<u>Public Interest</u>

The Act has a presumption in favour of disclosure. As a decision maker I am required to decide where, on balance, public interests lies. As part of this process I must consider factors favouring disclosure and non-disclosure.

In *Hogan v Hinch* (2011) 243 CLR 506, [31] French CJ stated that when 'used in a statute, the term [public interest] derives its content from "the subject matter and the scope and purpose" of the enactment in which it appears'. Section 17(1) of the Act sets out the test, to be applied to determine whether disclosure of information would be contrary to the public interest. These factors are found in subsection 17(2) and Schedule 2 of the Act.

Taking into consideration the information contained in the documents found to be within the scope of your request, I have identified that the following public interest factors are relevant to determine if release of the information contained within these documents is within the 'public interest'.

<u>Factors favouring disclosure in the public interest:</u>

(a) disclosure of the information could reasonably be expected to do any of the following:

(xiii) contribute to the administration of justice generally, including procedural fairness

Having considered the factor above, I consider that the release of these documents may contribute to the administration of justice generally, including procedural fairness by allowing you to have a record of the communications and decision-making process behind the investigation. I am satisfied that this factor favouring disclosure carries some weight. However, this factor is to be balanced against the factors favouring non-disclosure.

Factors favouring nondisclosure in the public interest:

(a) disclosure of the information could reasonably be expected to do any of the following:

x) prejudice intergovernmental relations;

When considering the documents and factors in favour of non-disclosure, I have considered that the release of the documents could prejudice intergovernmental relations. The documents identified provide details of confidential information shared between the ACT Government and other state governments. I am satisfied that the release of the documents could prejudice intergovernmental relations and the Directorate's ability to obtain confidential information by impairing the future flow of information between the ACT and interstate governments. I am satisfied that all factors favouring non-disclosure carry very significant weight.

(xii) prejudice an agency's ability to obtain confidential information.

An agreement to treat documents as confidential does not need to be formal. A general understanding that communications of a particular nature will be treated in confidence will suffice. The understanding of confidentiality may be inferred from the circumstances in which the communication occurred, including the relationship between the parties and the nature of the information communicated.

Having applied the test outlined in section 17 of the Act and deciding that release of confidential information contained in the documents is not in the public interest to release, I have chosen to redact this specific information in accordance with section 50(2). Noting the pro-disclosure intent of the Act, I am satisfied that redacting only the information that I believe is not in the public interest to release will ensure that the intent of the Act is met and will provide you with access to the majority of the information held by CMTEDD within the scope of your request.

Contrary to the public interest information under schedule 1 of the Act

Nine documents that have been identified as being within the scope of your request are either fully (documents 14-20 in the attached Schedule) or partially (documents 3 and 5 in the attached Schedule) composed of information that is considered to be contrary to the public interest information under section 1.2 of Schedule 1 of the Act as it is information that is deemed privileged under Legal Professional Privilege. This information can only be released if the parties involved agree to waive that privilege. The parties have not waived privilege.

Charges

Pursuant to *Freedom of Information (Fees) Determination 2018* processing charges are applicable for this request because the total number of pages to be released to you exceeds the charging threshold of 50 pages. However, the charges have been waived in accordance with section 107(2)(b) of the Act.

Online publishing – Disclosure Log

Under section 28 of the Act, CMTEDD maintains an online record of access applications called a disclosure log. Your original access application, my decision and documents released to you in response to your access application will be published in the CMTEDD disclosure log after three working days after the date of my decision. Your personal contact details will not be published.

You may view CMTEDD disclosure log at https://www.cmtedd.act.gov.au/functions/foi/disclosure-log-2020.

Ombudsman Review

My decision on your access request is a reviewable decision as identified in Schedule 3 of the Act. You have the right to seek Ombudsman review of this outcome under section 73 of the Act within 20 working days from the day that my decision is published in CMTEDD disclosure log, or a longer period allowed by the Ombudsman.

We recommend using this form *Applying for an Ombudsman Review* to ensure you provide all of the required information. Alternatively, you may write to the Ombudsman at:

The ACT Ombudsman
GPO Box 442
CANBERRA ACT 2601

Via email: actfoi@ombudsman.gov.au

ACT Civil and Administrative Tribunal (ACAT) Review

Under section 84 of the Act, if a decision is made under section 82(1) on an Ombudsman review, you may apply to the ACAT for review of the Ombudsman decision. Further information may be obtained from the ACAT at:

ACT Civil and Administrative Tribunal
Level 4, 1 Moore St
GPO Box 370
Canberra City ACT 2601
Telephone: (02) 6207 1740
http://www.acat.act.gov.au/

Should you have any queries in relation to your request please contact me by telephone on 6207 7754 or email CMTEDDFOI@act.gov.au.

Yours sincerely

Philip Dachs
Information Officer
Information Access Team
Chief Minister, Treasury and Economic Development Directorate

16 December 2020

ACT Government
Chief Minister, Treasury and Economic Development

FREEDOM OF INFORMATION REQUEST SCHEDULE

WHAT ARE THE PARAMETERS OF THE REQUEST	Reference NO.
Any documentary evidence such as Business Case, Procurement Plan Minute, Tender Evaluation Report or others that an open tender process was exercised. It not open tender, provide documents that justify why open tender wasn't an option.	CMTEDDFOI 2020-219

Ref No	Page number	Description	Date	Status	Reason for Exemption	Online Release Status
1	1-2	Email – i-Connect program – Customer Identity Management Service	19 Jul 2017	Full release	N/A	Yes
2	3-6	Email – i-Connect program - Customer Identity Management Service (Strategic Review)	15 Sep 2017	Full release	N/A	Yes
3	7-8	Email – I-connect	26 Sep 2017	Partial release	Sch 1 1.2	Yes
4	9	Minute to DG CMTEDD – Exemption from public tender document	6 Oct 2017	Full release	N/A	Yes
5	10-23	Attachment - Minute to above on Proposal to enter into a contractual arrangement – Exemption from public tender	6 Oct 2017	Partial release	Sch 1 1.2 Sch 2.2(a)(x)	Yes
6	24	Appendix D: CIDAM Market Intelligence	Undated	Full release	N/A	Yes
7	25-40	Emerging Vendors in the IDaaS Market	2 Nov 2016	Full release	N/A	Yes
8	41-69	Ovum Decision matrix: Selecting an Identity as a Service (IDaaS)	7 Dec 2016	Full release	N/A	Yes
9	70-100	Gartner Reprint - Magic Quadrant for Identity and Access Management as a Service, Worldwide	30 Nov 2016	Full release	N/A	Yes
10	101-109	iConnect Program - IDAM High- level evaluation	Undated	Partial release	Sch 2.2(a)(x)	Yes
11	110-115	Appendix E – Program Board Minutes	13 Jun 2017	Partial release	Sch 2.2(a)(x)	Yes
12	116-129	Appendix H – iConnect Digital Account Platform	28 Jul 2017	Full release	N/A	Yes
13	130-136	Government Procurement Board Strategic Review Submission	Undated	Partial release	Sch 2.2(a)(x)	Yes
14-20		Documents covered under LPP		Exempt	Sch 1 1.2	No
Total No of Docs						
20						

Subject: FW: i-Connect program – Customer Identity Management Service (Strategic Review)

Begin forwarded message:

From: "Althorp, Vanessa" <Vanessa.Althorp@act.gov.au>
Date: 19 July 2017 at 12:32:13 pm AEST
To: "Purser, Dave" <Dave.Purser@act.gov.au>
Cc: "Doran, Karen" <Karen.Doran@act.gov.au>, "Cumming, Jon" <Jon.Cumming@act.gov.au>
Subject: i-Connect program – Customer Identity Management Service (Strategic Review)

Hi Dave,

You are the nominated contact officer for the above procurement. Thank you for the proposal presented to the Board on the 11th July 2017.

The Board **noted** the presentation from the proponents, providing background and context for the procurement approach:

a. The original procurement strategy is no longer fit for purpose
b. A solution needs to be in place by the end of 2017 to ensure a WHOG approach, in particular a technical solution is needed by September 2017 to meet Education's project timelines
c. Going out to market will impact on timing of delivery of product

The Board **suggested** to the proponent that they

d. Consider the importance of a clear scope of works and detailed technical specifications to define the product/output expectations
e. Consider the basis for cost allocation to Directorates (pay on usage) and communication of this approach
f. Include further evidence that a single select provides value for money and other benefits
g. Include appropriate exit clauses in contract

The Board **noted** the Chief Digital Officer will bring the RFT to the Board for Stage Two.

Should you require clarification about this message, please contact me. If you wish to speak with a Board member about this decision, please contact Ms Karen Doran (Chair).

NOTE: It is the responsibility of the Project Officer to:

- Ensure that you are familiar with the Part 3 Notifiable Contracts requirements of the *Government Procurement Act 2001* including Section 26 Meaning of notifiable amendment, Division 3.3 Availability of notifiable contracts, and Division 3.4 on Confidential Text, and have planned to include the required information on the Contracts Register within 21 days after the contract is made. Refer to Procurement Circular PC16 Notifiable and Reportable Contracts at http://www.procurement.act.gov.au/About/procurement_circulars and the Contracts Register at http://www.procurement.act.gov.au/contracts
- Seek clarification immediately from the sender on the meaning of this message, if not absolutely clear;

- Advise all appropriate staff associated with the project of the Board's decision and any additional actions resultant from this advice;
- Should the process outlined above not commence within 3 months of this notice, provide a revised timetable;
- Complete all actions associated with this decision; and

Active Certification Officer
Phone: +61 2 6207 7352 |
Procurement and Capital Works | Chief Minister, Treasury and Economic Development Directorate | **ACT Government**
Macarthur House, Level 2 Annex, 12 Wattle Street Lyneham ACT 2602 |GPO Box 818 Dickson ACT 2602 | www.act.gov.au

From:	Colussi, David
To:	Glenn Powell [redacted]@synergygroup.net.au>; Smith, TraceyL
Subject:	FW: i-Connect program – Customer Identity Management Service (Strategic Review) [SEC=UNCLASSIFIED]
Date:	Friday, 15 September 2017 9:23:32 AM

Regards David

From: Colussi, David
Sent: Friday, 15 September 2017 9:23 AM
To: Whitten, Meredith <Meredith.Whitten@act.gov.au>; Cumming, Jon <Jon.Cumming@act.gov.au>
Cc: Althorp, Vanessa <Vanessa.Althorp@act.gov.au>
Subject: RE: i-Connect program – Customer Identity Management Service (Strategic Review) [SEC=UNCLASSIFIED]

Thanks Meredith

Just to confirm I am on the same page:

We will do the second pass out of session and provide:

1. The single select minute updated to include the feedback of our meeting on Tuesday
2. The RFQ documentation requested in the highlighted string below

Couple of questions:
Is there anything else I need to provide?
Can I relinquish the slot at GBP we have scheduled for 9am this coming Tuesday (19th)?

Thanks for driving the process on for us. Much appreciated.
Regards David

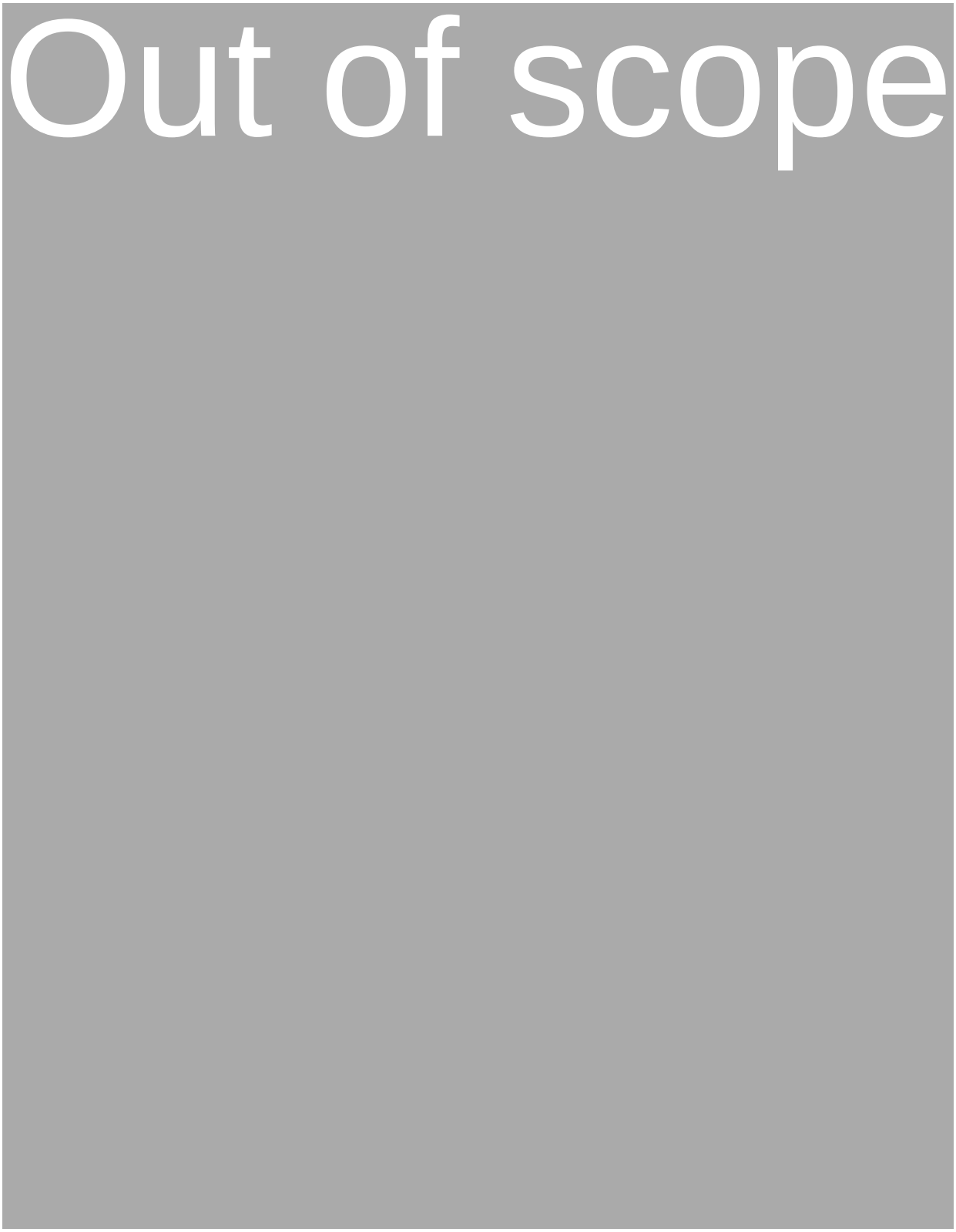
From: Whitten, Meredith
Sent: Thursday, 14 September 2017 10:26 PM
To: Cumming, Jon <Jon.Cumming@act.gov.au>; Colussi, David <David.Colussi@act.gov.au>
Cc: Althorp, Vanessa <Vanessa.Althorp@act.gov.au>
Subject: RE: i-Connect program – Customer Identity Management Service (Strategic Review) [SEC=UNCLASSIFIED]

Hi Jon

The Board was addressing the current proposal for a second pass.
Very happy for you to send through the single select documentation for the Board to consider.
I will see if we can do that out of session.

Many thanks

Meredith Whitten | Deputy Director-General |
Phone 620 70384 | Mobile 0419 426 308
Business Services Division | Education Directorate | **ACT Government**
Level 1 Annex 220 Northbourne Avenue Braddon ACT 2601 | GPO Box 158 Canberra ACT 2601 |
www.act.gov.au |www.det.act.gov.au | Facebook | Twitter | Pinterest | LinkedIn | Google+



Out of scope

Out of scope

From:	Colussi, David
To:	Russell Baker Sch 2.2(a)(ii) @iconnectdigital.net>; Glenn Powell Sch 2.2(a)(ii) @synergygroup.net.au>; Corby, Leila; Smith, TraceyL
Subject:	FW: I-connect [SEC=UNCLASSIFIED, DLM=For-Official-Use-Only]
Date:	Tuesday, 26 September 2017 1:03:37 PM
Attachments:	image003.emz image004.png

From: Althorp, Vanessa
Sent: Friday, 22 September 2017 12:09 PM
To: Colussi, David <David.Colussi@act.gov.au>
Cc: Whitten, Meredith <Meredith.Whitten@act.gov.au>; Bailey, Kylie <Kylie.Bailey@act.gov.au>; Cumming, Jon <Jon.Cumming@act.gov.au>
Subject: I-connect

Hi David,

You are the nominated contact for the above procurement. Thank you for the proposal presented to the Board on the 19th September 2017.

The Board **noted** the presentation from the proponents, providing background and context for the procurement approach:

a) The timing of this procurement is imperative to keep Directorates engaged

b) A clearer scope of works and detailed technical specifications has been included to define the product/output expectations

Sch 1 1.2

d) The risks are being managed through the Project Board

The Board **suggested** to the proponent

a. Liaise with Goods & Services;

Sch 1 1.2

The Board **asked** for the risk plan to be provided to them.

The Board **endorsed** the Chief Digital Officer proposing a single select to The Head of Service to engage Saleforce for a period of three years to the value of $.099 million.

Should you require clarification about this message, please contact me. If you wish to speak with a Board member about this decision, please contact Ms Meredith Whitten (A/g Chair).

NOTE: It is the responsibility of the Project Officer to:

- Ensure that you are familiar with the Part 3 Notifiable Contracts requirements of the *Government Procurement Act 2001* including Section 26 Meaning of notifiable amendment, Division 3.3 Availability of notifiable contracts, and Division 3.4 on

Confidential Text, and have planned to include the required information on the Contracts Register within 21 days after the contract is made. Refer to Procurement Circular PC16 Notifiable and Reportable Contracts at http://www.procurement.act.gov.au/About/procurement_circulars and the Contracts Register at http://www.procurement.act.gov.au/contracts

- Seek clarification immediately from the sender on the meaning of this message, if not absolutely clear;
- Advise all appropriate staff associated with the project of the Board's decision and any additional actions resultant from this advice;
- Should the process outlined above not commence within 3 months of this notice, provide a revised timetable;
- Complete all actions associated with this decision; and

Thanks
Vanessa

MINUTE

ACT Government
Chief Minister, Treasury and Economic Development

Date 6th October 2017

To Kathy Leigh, Director-General
- Sue Hall, Executive Director, Corporate

From Jon Cumming, Chief Digital Officer

Exemption from public tender

Proposal to enter into a contractual arrangement with

Salesforce for a Digital Platform (iConnect).

Exemption from public tender ($200,000 or more)

under the Government Procurement Regulation 2007 (Regulation)

MINUTE

ACT Government
Chief Minister, Treasury and Economic Development

Date	6th October 2017	TRIM No: File No: 2017/1250
To	Kathy Leigh, Director-General • Sue Hall, Executive Director, Corporate	
From	Jon Cumming, Chief Digital Officer	
Subject	**Proposal to enter into a contractual arrangement with Salesforce for a Digital Platform (iConnect) - Exemption from public tender *($200,000 or more)* under the Government Procurement Regulation 2007 (Regulation)**	

Critical reason and date

1. This Minute seeks your exemption from conducting a public tender process and to conduct a single select tender process.
2. **September/October 2017** to be able to secure a contract with Salesforce that enables the Digital Platform (as part of the iConnect Program) to be ready for release to production to meet urgent needs of agencies including Revenue, Access Canberra and the Education Directorate.

Summary

3. The ACT Digital Strategy 2016-19 requires pursuit of cloud solutions and preferably SaaS where available. In adopting SaaS solutions, security certification from the Australian Signals Directorate (ASD) is required to meet the SSICT CDAF framework. Only two providers have ASD certification for SaaS provision: Salesforce and Microsoft. Of these two, only Salesforce has demonstrable capability and capacity delivering cloud-based identity management with Microsoft only entering the identity SaaS market in early 2017.
4. The iConnect Program has established a production-ready Minimal Viable Product (MVP) of the Salesforce solution. This is a low-cost MVP proving the architecture, security robustness and technical capability required to support a full deployment across ACT Government.
5. This procurement seeks to extend the MVP licensing arrangement to support production volumes with a three-year contract with Salesforce.
6. The iConnect Program has approached Salesforce with a set of requirements. The quote received is $0.99m over three years. As a comparison of value for money, the original approach to the open market in 2014 yielded responses with total cost of ownership over three years of between $3.049m to $12.160m.

Background

7. In March of 2015 a Procurement Plan Minute (PPM) was approved together with an amendment minute. Collectively these documents set the framework for a procurement process (under the $21.8M iConnect budget) of $15.875M. The spend to date under that PPM is $4.757M. The PPM and amendment are attached as Appendices F & G respectively.

8. iConnect went to market in 2015 for solutions with a:

   - Request for Proposal for "Provision Of Technology Platforms for the iConnect Program [2014.25016.110] - Customer Experience (CE), Customer Identity and Access Management (CIDAM) And Enterprise Integration (EI)"; and
   - Request for Quote (RFQ) for "Provision of System Integration Services [25016.111] – Customer Experience (CE) and Customer Identity and Access Management (CIDAM) - Wave 1".

9. The following were selected as providers for the work and contracts were prepared as follows:

   - Sch 2.2(a)(x) [executed 30/09/2015]
   - Sch 2.2(a)(x) [executed 02/10/2015]
   - Sch 2.2(a)(x) [no contract executed, procurement process terminated]
   - Sch 2.2(a)(x) [executed 29/03/2016]. This procurement process in this instance was an RFQ. It should be noted that iConnect was unable to negotiate a satisfactory outcome-based Statement of Work for the provision of integration services for the CIDAM component.

10. Despite the selection process being fully compliant and robust against the applicable procurement standards, the outcome has been poor:

    - Cloud is still a brave new world with a relatively small critical mass of buyers. Consequently, the contract bargaining power rests with vendors and contracts are by and large 'take it or leave it' affairs, focussed on buyer obligations and vendor rights and disclaimers. Negotiations can be challenging and drawn out as evidenced in the recent renegotiation of the Territory Microsoft cloud contract.
    - The contracts executed had little flexibility and were built on the assumption that all the contributors to the project would successfully deliver the outcome. Cost commitments and contractual obligations were locked in at execution date in favour of the suppliers.
    - There were no termination for convenience clauses for the licences. The only grounds for termination were insolvency of the vendor(s) and un-remediated

material breach of contract, noting that the concept of a "material breach" is undefined in the contracts (GSO advice #631524, 20.12.2016).

- The contracts contained very little of the 'evidence' provided in the tender response – and so no commitment to deliver to the tender response. Thus non-delivery to the evidence provided in the tender response did not constitute a breach of contract.
- The low level of project definition meant that the initial execution and work delivery was based on 'time and materials' or equivalent. By the time the work was sufficiently framed to be outcome-based, there was no longer any competitive tension, and the quotations contained such a premium on time and materials that it was clear the project goals could not be achieved within the authorised budget.
- As the external review into the iConnect Program notes, the procurement approach resulted in a situation where the implementation partner did not underwrite the solution; that partner "...held no responsibility for any problems with the solution because it was chosen by the client. This is a very high risk approach as systems integration costs are unpredictable, frequently resulting in massive budget and schedule overruns" (iConnect Program Review, 30.11.16, p3).

11. Whilst there are many learnings from this, the critical one at this juncture is that traditional tender responses and evaluation as executed in this case were, in retrospect, a very unreliable indicator/guarantee of a good outcome. To understand whether a solution is viable it is seemingly necessary to build or acquire a prototype into a development environment as a minimum. There are too many environmental and product variables to rely on a desktop/artefact-based selection.
12. These lessons have been adopted by the iConnect Program as evidenced by the approach to the Sch 2.2(a)(x) option below.

Program Review and Refocus

13. As a result of the circumstances and outcomes outlined above, an independent review of the iConnect Program was commissioned in September 2016.
14. The review recommended focussing on the development of a foundational CIDAM solution, being the essential component required by directorates to progress their digital transformation projects.
15. A market scan of CIDAM options took place and in February 2017, and the iConnect Program Board agreed to an initial path of exploring the Sch 2.2(a)(x) CIDAM as a service. The due diligence process entailed alignment with, and exploration of, the Sch 2.2(a)(x) technology stack, including its use of Salesforce as a customer experience platform.

Sch 2.2(a)(x)

The Path Forward

22. As a result of the finding that the Sch 2.2(a)(x) was unsuitable, the iConnect Program Board considered three options proposed by the program for the path forward to implement a CIDAM:

    i. Just stop – wind the Program up immediately

    ii. Hard pause – suspend all Program activities except an environmental scan; resume program when CIDAM market has matured

    iii. Proceed with Salesforce delivering the CIDAM

23. The Program Board endorsed the third option – to proceed with a Salesforce CIDAM – noting some critical influencing factors:

    a. The Salesforce-based CIDAM developed during the due diligence process had been demonstrated to work in live demonstrations to key directorates requiring CIDAM for their digital transformation projects,

including Access Canberra, ACT Revenue and the Education Directorate[1]. The Salesforce CIDAM is now at a point where there is a production-ready MVP, and strong evidence that functionality required beyond the MVP could similarly be provided in Salesforce. The Salesforce CIDAM delivers against the MVP requirements to provide:

- Level 2 verified identity for a citizen
- authenticated and trusted citizen accounts that directorates can use
- the ability for citizens to access directorate systems using a single account (Single Sign-on)
- the ability for the CIDAM to 'know' the customer, delivering on the ACT Digital Strategy direction of 'tell government once' whilst complying with the *Information Privacy Act 2014 (ACT)*
- secure, supported and standards based services; the approach aligns to the ACT Digital Strategy, and the Program Review recommendation for a SaaS based and customer centric solution.

b. Multiple directorates have an urgent need for a CIDAM (Appendix B summarises the directorate CIDAM requirements). If CIDAM is not provided in a timely way by iConnect, each directorate will provide separate identity solutions and therefore multiple individual identities for citizens. This will require each directorate to invest in building their own standalone CIDAM, duplicating effort and costs.

c. In this event, citizens would create multiple identities across directorates. Re-combining these at a later date and merging them would be a complex and costly manual process requiring the build of toolsets to identify different accounts belonging to a particular user. There is a real risk that inappropriate merging could result in privacy breaches (two people using the same email address for different purposes).

d. Critical in this is that the individual directorate identities would not have the ability to manage (a common) Level 2 verification (Appendix C explains the levels of verification). This is required to create certainty that a user is indeed who they say they are. In short, if multiple identity options were built across directorates, they could not simply be 'reverse federated' with Level 2 verification associated with them. It has to be from the centre out as executed by iConnect.

e. An open market test in the short term would be highly unlikely to produce a better value for money solution as the market is demonstrably immature as outlined in Appendix D. Furthermore, there was insufficient

[1] The Program Board membership includes the DDG of Education, the Revenue Commissioner, and the DDG of Access Canberra

time to conduct an open market test given the urgent requirements of directorates. The Program Board was of the view that if an open tender was required, the project should halt as it could not achieve the project goals in a timeframe suitable for directorates with pressing CIDAM requirements in their digital transformation projects.

f. The experience of the iConnect team with the previous tender process highlights the need to take short listed tenderers through to a functional and live MVP to validate a vendor selection. This comes with an associated time, cost and internal resourcing challenge. Market information suggests that the market is rapidly maturing. At this time there are few reliable providers of suitable platforms, but indications are that in two years there will be genuine choice (Appendix D summarises intelligence on the CIDAM market).

g. The Australian public sector eco-system for CIDAM is also maturing. Ongoing initiatives including those of the Australian Government's Digital Transformation Agency (with GovPass) are likely to see a period of flux, potentially resolving in opportunities for policy alignment and platform sharing to the benefit of the Territory and its citizens. A market test in two years will be able to take advantage of this increased maturity.

24. Intrinsic to its endorsement of the Salesforce CIDAM solution, the Program Board endorsed a single select procurement approach for the interim MVP period (the minutes of the relevant Program Board meeting are Appendix E).

25. Note that this proposal for an exemption from a public tender process applies only to the subscription licensed product of Salesforce (with a clear exit path through ceasing the subscription). (See paragraphs 36 and 37 for further detail.)

26. Where build and other services associated with Salesforce technology are required for the iConnect Program, relevant contractors will be engaged through an open and appropriate procurement process. At present this is done through the contractor portal, but there is an intention to move to a more strategic supplier relationship – most likely with multiple vendors.

27. Finally note that reference to 'Salesforce' is generally a reference to Salesforce.com Singapore Pte Ltd.

Suitability of Salesforce

28. The selection of Salesforce was not arbitrary. It was primarily adopted because it has been selected by Sch 2.2(a)(x) for their CIDAM, and its use was intrinsic to the Sch 2.2(a)(x) the Territory. It was therefore used for the CE layer to replicate the Sch 2.2(a)(x) .

29. Salesforce is also being adopted across other states and territories for customer experience and CIDAM, including in the South Australian and Victorian State Governments (see eg http://www.themandarin.com.au/80527-service-victoria-alpha/).

30. Salesforce at the time of the market scan was the only SaaS CIDAM platform that was accredited by the ASD to securely host the Personal Information that is to be supplied by citizens. Previous negotiations with Salesforce have included incorporating their adherence to applicable privacy principles when processing customer data, further providing assurance that privacy safeguards are designed into the solution.

31. The product is considered 'leading' in an emerging market of similar products, as indicated by the Gartner and Ovum analysis of the CIDAM market, summarised in Appendix D.

32. Additionally, the Board requested an independent assessment to validate the suitability of the Salesforce platform to deliver the required capabilities. Accenture engaged and "found that Salesforce is a suitable platform to deliver the intended services." (see Appendix H)

Period of proposed MVP CIDAM covered by single select procurement

33. Research by both Ovum and Gartner identifies that the CIDAM space is changing rapidly, with many new entrants and developing products on the market and significant maturity gained in the next two years (Ovum: Emerging Vendors in the IDaaS Market; Gartner, Magic Quadrant for Identity and Access Management as a Service, Worldwide).

34. On this view, in two years the market response to a tender would result in more credible responses including from Sch 2.2(a)(x) . These could be taken to MVP in development (as a Service) as part of the evaluation.

35. It is therefore proposed that the procurement cover a **maximum three year period** of MVP CIDAM delivered by Salesforce. Within this period a full market test will be conducted to take advantage of the matured CIDAM market.

Out of scope

Reason/s for Request for Exemption and Details of Proposed Contract

41. Section 9 of the *Government Procurement Regulation 2007* requires a Territory entity to invite public tenders for the procurement of goods, services or works if the total estimated value of the procurement is $200,000 or more.

42. The required services are Salesforce licences to the total value of between $0.99m and $1.2m (GST inclusive) over the course of a proposed three year contract.

43. As discussed above at paragraph 27, the supplier identified for this procurement is Salesforce.com Singapore Pte Ltd.

44. The Regulation provides that the responsible chief executive officer may, in writing, exempt the entity [from the market test requirement] only if satisfied, on reasonable grounds, that the benefit of the exemption outweighs the benefit of compliance with the requirement [Government Procurement Regulation 2007, section 10 (1) and (2)].

45. It is the contention of the iConnect Program that there are reasonable grounds to confidently assert that the benefits of the exemption (authorising the procurement of Salesforce to support the interim MVP) outweigh the benefits of compliance with the requirement for a market test. The reasons being that:

    a. There is only one sufficiently mature provider in the market place at this time. Going to market will not attract any suitable responses. A competitive and mature market in this technology space is expected to evolve over the 2 years. (see para 23g, 33-35)

    b. Equally, going to market will not attract any better value for money responses (see para 23e, 28-32)

    c. Going to market for a full open tender will over-reach the Program's timeframe to deliver CIDAM. (see para 23e)

    d. Not proceeding with the interim MVP CIDAM using Salesforce via a single select, and in light of the above, will render the iConnect Program

untenable and as a result the majority of the accrued asset value ($10M being the cost of the MVP and the settled commitments to the unfulfilled contracts referred to in paragraph 9) will be written off. (see para 23b)

e. Not proceeding with the interim MVP CIDAM using Salesforce via a single select tender process will create a technical debt through dispersed level 1 verified identities which are complex to recombine accurately and without privacy risk. (para 23d)

f. Should this exemption from a public tender process not proceed each directorate will need to build their own CIDAM solution, fragmenting the experience for Citizens as they engage across directorates. Conservative estimates of each directorate developing a standalone CIDAM is in the ball park of $1M per directorate, excluding respective software licenses. This excludes costs associated with delays within directorates associated with any delays incurred waiting for CIDAM development to be undertaken. The Territory will incur a greater aggregate cost as directorates individually replicate a number of identity solutions for their project needs. (see para 23b)

g. Without this solution, citizens will have to obtain Level 2 identity accreditation multiple times with different directorates. (see para 23b)

h. The exemption from a public tender process is to cover a short term procurement of three years, within which time a full market test will be completed in full compliance with the procurement regulation. The short term nature of the procurement reduces the impact to government of any 'value for money' downside, and ameliorates a market perception of uncontested technology lock-in. (see para 23g, 35)

46. This request seeks your agreement as the "responsible chief executive officer", that the above collectively represents reasonable grounds "that the benefit of the exemption outweighs the benefit of compliance with the requirement" [*Government Procurement Regulation 2007*, section 10 (2)].

47. The proposed duration of the contract is one year with two 'plus one year' extension options, subject to funding and performance.

48. The estimated value, GST included, of the proposed base level procurement is $0.99m over three years. To account for the possibility of faster acceptance and uptake by citizens than projected and the resulting growth in use of the CE and CIDAM, the iConnect Program requests additional headroom in the procurement threshold, should the need arise, of up to 20% of the above total (an extended total of $1.2m).

Value for Money

49. If you authorise this exemption, I will arrange for a procurement process to be conducted as prescribed to consider value for money (under s22A of the *Government Procurement Act 2001*).

50. This value-for-money assessment will be presented to you for sign off as the delegate.

51. On your agreement that the procurement represents value for money, a contract will be negotiated with the proposed supplier/contractor only if I am satisfied that:

    (a) the resultant contract is confirmed to deliver demonstrable value for money to the Territory, and

    (b) relevant due diligence has been satisfactorily completed in relation to the supplier/contractor.

52. The proposed contract will be signed on behalf of the Territory by the appropriate delegate – or provided to you for your authorisation to maintain consistency in the process – as you determine to be appropriate.

Consultation

53. The Government Procurement Board (GPB) was consulted on 11 July 2017 and appraised of the approach. GPB **noted**:

    a. The original procurement strategy is no longer fit for purpose
    b. A solution needs to be in place by the end of 2017 to ensure a WHOG approach, in particular a technical solution is needed by September 2017 to meet Education's project timelines
    c. Going out to market will impact on timing of delivery of product

GPB **suggested:**

    a. Consider the importance of a clear scope of works and detailed technical specifications to define the product/output expectations
    b. Consider the basis for cost allocation to directorates (pay on usage) and communication of this approach
    c. Include further evidence that a single select provides value for money and other benefits
    d. Include appropriate exit clauses in contract

54. In reference to the above suggestions the iConnect Program confirms:

    a. There is no build work required of Salesforce. Salesforce is a SaaS product meaning the platform is a complete product to which we are seeking access through a licensing agreement. There is no scope of work for Salesforce to undertake and the technical specification of the product already exists as part of the Salesforce documentation suite. The guarantee of output/outcome was confirmed with the successful MVP.

    b. The model of cost allocation for the iConnect platform is being considered under the remit of the iConnect Program Board.

c. There has been a comparative analysis of cost (see paragraph 6), and a comprehensive assessment of suitability and value (see paragraphs 28-32).

Sch 1 1.2

55. On 19 September 2017 GPB considered this Minute and the RFQ. GPB **noted** the presentation from the proponents, providing background and context for the procurement approach:

a) The timing of this procurement is imperative to keep Directorates engaged,
b) A clearer scope of works and detailed technical specifications has been, included to define the product/output expectations,

Sch 1 1.2

d) The risks are being managed through the Project Board.

GPB **suggested** to the proponent:

a. Liaise with Goods & Services,

Sch 1 1.2

GPB **asked** for the procurement risk plan to be provided (completed); and **endorsed** the Chief Digital Officer proposing a single select to the Head of Service to engage Salesforce for a period of three years to the value of $0.99 million.

Sch 1 1.2

Financial

57. iConnect has funding of $6.9m in 2017-18; and $1.7m in 2018/19. The value of the procurement activity in this brief is covered by available program funding.

Risks/ Sensitivities

58. **Limited test of value for money**
Not approaching the market limits the understanding of market prices. To mitigate this risk the iConnect Program has approached Salesforce with a set of requirements. The indicative cost is anticipated to be approximately $0.99m over three years. As a comparison of value for money, the original approach to the open market in 2015 yielded responses with total cost of ownership over three years of between $3.049m to $12.160m.

Subject to your authorisation of this exemption request, I will arrange for a

procurement process to be conducted as prescribed to consider value for money (under s22A of the *Government Procurement Act 2001*).

59. **Risk of procuring a poor product**
Competitive tendering is usually utilized to promote the best procurement outcome. This risk has been mitigated by establishing a low cost, small scale yet fully functioning version of the solution. This version has been fully developed, integrated and tested and found suitable. The product was also independently assessed by Accenture who found it suitable for the purposes as stated by the Territory.

60. **Complaint from competitor**
As with any single sourcing arrangement, there is the potential for scrutiny of this decision (as is appropriate), recognising it is important to balance any concerns with the imperative to deliver the necessary service foundation to directorates. There are strong grounds to confidently defend that the benefits of the exemption outweigh the benefits of compliance with the requirement for a market test. These are listed at paragraph 45.

61. Risk of not proceeding.
There is significant risk of not proceeding with single select at this time (para 45). In summary, these are:

    a. write off of the accrued asset value to date (approximately $10m),
    b. creation a technical debt through dispersed level 1 verified identities which are complex to recombine accurately and without privacy risk,
    c. each directorate will need to build their own CIDAM solution duplicating efforts, systems and costs and fragmenting customer experience,
    d. citizens will have to obtain Level 2 identity accreditation multiple times with different directorates.

Media

62. Nil.

Recommendations

That you:

- approve this request for an exemption under s10 of the Regulation to not invite public tenders, and

AGREED/NOT AGREED/PLEASE DISCUSS

- direct the OCDO to invite a tender from Salesforce.com (or a related body corporate) for the procurement of a Digital Platform (up to the value of $1.2m (GST inclusive) over three years) in order to assess value for money. Once the tender is assessed you as delegate will be presented with the assessment for

your consideration and, if applicable, authorisation to enter negotiations for a contract (or enter a contract if no negotiations are required).

AGREED/NOT AGREED/PLEASE DISCUSS

Kathy Leigh..... 16/10/17

Jon Cumming

Action Officer: David Colussi, Director Digital Experience

Phone: x 70215

Director-General's Response, Reasons and Direction/s (if any)

With respect to the procurement proposal outlined in this Minute, I do/do not agree to grant an exemption under s10 (1) of the Regulation on the justification given in the Minute, and for the following reason/s (if any):

Option 1. Exemption is granted/reasons:

As set out in part 6 of the attached minute, in particular reasons (a) + (b)

Directions: CMTEDD will:

(a) invite a tender from the proposed supplier/contractor referred to in this Minute

(b) instead of a single select procurement methodology, seek the following kind and/or number of quotations for the procurement:

.....

.....

(c) other:.....

.....

Only proceed to a contract if the outcome of an assessment of the tender demonstrates value for money.

Option 2. Exemption not granted/reasons

.....

.....

.....

Directions:

(a) conduct a public tender process - OR

(b) do not proceed with this procurement and discuss options with me

Kathy Leigh..... 16/10/17

Director-General
Chief Minister, Treasury and Economic Development Directorate

Appendix D:
CIDAM Market Intelligence

Ovum
TMT intelligence | informa

Emerging Vendors in the IDaaS Market

Identity-as-a-service attracts big guns as well as smaller specialists

Publication Date: 02 Nov 2016 | Product code: IT0022-000809

Rik Turner

Summary

Catalyst

Ovum regularly carries out vendor comparison projects under the collective title of Ovum Decision Matrix (ODM) reports. The Security team is finalizing an ODM on the identity-as-a-service (IDaaS) market, in which identity services that would traditionally fit under the identity and access management (IAM) banner are offered from the cloud, involving no deployment of on-premise software. While the report itself compares eight vendors, so many other companies are in "the identity conversation" in one way or another, and we have decided to devote a separate report to them. The reason for this is that some of them are so big, with so much tech industry clout, that they have the potential to profoundly disrupt what is still an emergent section of the identity service market. Others are still small, but their focus on the B2C side of identity services leads Ovum to believe that they are destined for bigger things.

Ovum view

As the ODM on IDaaS shows, this is a growing segment within the broader identity and access management (IAM) market for a couple of reasons.

First, traditional IAM involves the installation of on-premise software, which is often a lengthy and expensive process that entails a considerable amount of professional services to customize the technology to customer-specific requirements, thereby putting it beyond the pocket of all but the largest enterprise customers. A cloud-based service offers the promise of replacing capital expenditure with operating expenditure, with the added benefit of the scalability and flexibility that the cloud can bring.

Second, enterprise functionality, in the form of the applications used in the business, is increasingly moving into the cloud. At the same time, more and more corporate employees are working remotely, while entire business processes are being outsourced to third parties, often in completely different geographies. All of this makes identity services delivered from the cloud a compelling alternative to on-premise software.

This scenario has, of course, not gone unnoticed by some of the heavyweights in the tech industry, so while several of the companies featured in the upcoming ODM on IDaaS are start-ups that came into existence specifically to deliver identity services from the cloud, the market has now expanded to a point where other, larger entities are joining the fray. Some of these, such as IBM and Microsoft, felt ready to stand up their services for comparison with the specialists, and so are featured in the ODM. Others are at an earlier stage, having only recently come into the market.

These companies appear in this ancillary report, alongside a smaller group of specialists that focus exclusively on customer IAM (CIAM). We recommend that you scan all the profiles in the report to familiarize yourself with what all these companies are thinking and doing about IDaaS. Ovum sees the cloud as the future of IAM, with B2C the driver for new IAM functionality. The companies in this report are the ones to watch as the market moves forward.

Key messages

- The IDaaS marketing is expanding.

- Some big names are circling the IDaaS market.
- CIAM specialists are also thriving.

The IDaaS marketing is expanding

Our main ODM report on IDaaS looks at vendors in the IDaaS market that fall into one of two categories.

On the one hand, there are what we might term the "cloud-native" companies that came into existence to create a cloud-based identity management platform for delivery as a service. On the other, there are the companies with a heritage in on-premise IAM systems and that have moved, either through acquisition or through internal development, into IDaaS to complement their existing identity management business.

Companies in the first category include the likes of Okta, Ping, Centrify, and OneLogin, while the second category includes companies such as IBM, which bought into the space with its 2014 acquisition of Lighthouse, and Microsoft, a long-term participant in identity management via both its Active Directory and Forefront products. Another company in the main report, SailPoint, actually started on-premise, but moved fairly quickly into the cloud, and so is not an IAM "incumbent" in the way that IBM and Microsoft are.

This Emerging Vendors report, meanwhile, is about companies that did not make it onto the list of those subjected to our full examination for the vendor comparison process, but that we nonetheless consider worthy of our readers' attention in this sector. One IAM incumbent, Oracle, is moving into the IDaaS market, but was not quite ready to submit to the full comparison process, and for this reason it appears here.

Also in this section, we profile some of the smaller, dedicated IDaaS players that are focused primarily on the business-to-consumer side of the market, describing what they provide as customer identity and access management (in the case of Janrain) or customer identity management (Gigya).

Another group featured in this section are major industry players that are neither traditional IAM vendors nor IDaaS startups, but which by virtue of their clout elsewhere in the hi-tech sector are well placed to move into cloud-based identity management, and in some cases are already doing so, now that more and more business and consumer interactions are being conducted online. Some of them are big web properties, such as Amazon Web Services (AWS), Salesforce.com, and Google. Another is VMware, a major player in on-premise infrastructure that aims to catch up with the other big names in the cloud market. Not all of these companies are focused on the enterprise identity market, but they all have the potential to make a significant impact on the segment, given the sheer numbers of employees and/or consumers they interact with on a daily basis.

Furthermore, they already manage identities to enable customers to access their services, whether they be AWS's infrastructure-as-a-service cloud offerings, Salesforce's online CRM, or Google's Apps. As the market leader in server virtualization, VMware also has extensive expertise in managing identity-based access to environments around the world that use its hypervisor technology, an experience that informs the VMware Identity Manager service it launched in mid-2015.

As such, any of these IT industry behemoths could make the jump from managing identities for customers to get to their services to offering identity services for accessing any application, online or

on-premises, theirs or a third party's. At that point, they become a competitor in IDaaS, and some already have.

Some big names are circling the IDaaS market

Salesforce

Salesforce has been in the IDaaS market since October 2013, when it launched theSalesforce Identity service.

With the tagline "Identity for a Connected World", Salesforce Identity is targeted at all the major use cases of identity services, including business-to-employee (B2E), business-to-business (B2B), and business-to-consumer (B2C). When announcing its availability, Salesforce said the service was designed to enable CIOs "to deliver a simple, productive, and customized user experience across every web, mobile, and on-premises app".

In moving into identity services, Salesforce is seeking to leverage its strength in the world of customer relationship management (CRM), in that it provides the system of record for customers, contacts, and customer-related business processes for more than 150,000 companies around the world.

It argues that CRM is itself going through digital transformation, where direct human interactions with customers are increasingly being replaced by digital ones, whether on the web, in mobile applications, or through connected devices and IoT, making identification a core competency. Having built identity into its CRM platform clearly brings benefits to Salesforce customers, but it was also logical for it to roll out a service that can be acquired as a standalone, even by companies that are not existing Salesforce customers.

The logical first place to start marketing such a service is, however, as an upsell into its existing customer base, where the relationship with Salesforce already exists, and extending identity services out beyond Salesforce applications will further sediment Salesforce in the account. Indeed, the company argues that selling Salesforce Identity into such customers is not even an IAM conversation in the traditional sense.

For existing customers, the fee for the Identity service is bundled into the customer's overall Salesforce license, though separate licenses for Salesforce Identity license as a standalone. Pricing for B2E and B2B is per user, per month, while for B2C usage, it can be by the number of active users each month.

Like other Salesforce services relating to security, such as the Shield encryption capability, Salesforce Identity is underpinned by the company's app cloud platform-as-a-service (PaaS) capability. This makes it customizable by Salesforce customers, such as, for example, for purposes of branding it as their own identity service for particular constituencies, such as employees or customers. Salesforce view identity standards as a key way of removing risk from integrations and deployments, and participates heavily in standards bodies. Salesforce Identity supports several open standards, including:

- **SAML**: an XML standard that allows secure web domains to exchange user authentication and authorization data

- **OAuth**:a standard for token-based authentication and authorization on the Internet, which allows an end user's account information to be used by third-party services without exposing the user's password
- **OpenID Connect**: a simple identity layer on top of the OAuth 2.0 protocol that allows computing clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end user in an interoperable and REST-like manner
- **SCIM**: a standard for automating the exchange of user identity information between identity domains or IT systems.

The Salesforce Identity service has various components, including Salesforce Identity Connect, single sign-on (SSO) and provisioning, and multi-factor authentication.

Salesforce Identity Connect

This is an identity bridge that sits on a customer's premises to provide integration with any local Active Directory so that users, attributes, entitlements, single sign-on, and identity federation can be extended across both on-premise and cloud environments. Identity Connect is charged for separately from the remainder of the service, with customers typically paying a per-user, per-month add-on.

Single sign-on (SSO) and provisioning

This capability improves usability and security with standards-based single sign-on for any web, mobile, or on-premise app. When combined with multi-factor authentication (MFA) and federation services, SSO enables a seamless access experience across cloud and on-premise apps, as well as across multiple companies' applications.

To this end, Salesforce Identity also supports social sign-on, meaning that users can bring their identity from public providers such as Facebook, Google, Amazon, and Paypal. The service also supports self-registration (self-provisioning), which is vital if identity services are to be extended, particularly to the B2C environment.

Multi-factor authentication

While Salesforce Identity provides an out-of-band contextual MFA for Salesforce's own services, the facility can also be used for applications, whether from third parties or developed by customers themselves.

The company's offerings in this context were bolstered earlier this year when it added a push-based authentication capability. This was the result of its 2015 acquisition of Toopher, a company which had developed an Android and iOS app that authenticates a user's identity by accessing the mobile device's location information.

Expect further investment in MFA for the service. In its upcoming Winter 17 release, the company will offer support for FIDO U2F-compliant hard tokens and temporary tokens, as well as delegated administration.

Amazon Web Services

Amazon Web Services (AWS) is the absolute leader in cloud infrastructure services. Its estimated market share of 31% in the second quarter of 2016 outstripped the combined shares of its next three

competitors: Microsoft (11%), IBM (5%) and Google (8%). AWS also has 10 times more computing capacity than the next 14 cloud providers combined.

The company, which is a division of online retailing giant Amazon, is 10 years old this year. Launched in March 2006, its first two infrastructure-as-a-service (IaaS) offerings were for compute (EC2) and storage (S3).

AWS's forays into the world of identity management have so far been designed to enhance its now considerably expanded portfolio of IaaS offerings, which is logical, given that more than a million active users log on to these each month.

As organizations move their data centers into the cloud, they need robust platforms equivalent to traditional IAM tools to manage access to the cloud-based resources. However, AWS sees extending existing IAM tools for this purpose as challenging, because these tools do not scale, due either to lack of integration or to the complexity of the new environment. As a result, AWS identified the need for a new approach, and sought to address this requirement by building a native IAM layer into its platform.

AWS IAM

In 2010, the company added an IAM service that allows customers to assign permissions to their system administrators and their applications to gain access to the AWS resources in their accounts. IAM users can be granted permission to launch an EC2 instance, but the same user/credential cannot be used to log into (in Windows) or SSH into (in Linux) that instance.

As the company explains it, AWS IAM allows customers "to manage access to compute, storage, database, and application services in the AWS Cloud", leveraging the conventional IAM concepts of users, groups, and permissions applied to individual API calls to control which users can access which services and so on, the kinds of actions they can perform, and which resources are available to them. The kinds of assets and actions that are governed include everything from virtual machines (VMs), which are the bedrock of AWS's processors-for hire service EC2, to the databases instances a company has on AWS, and the ability to filter database query results.

AWS Directory Service

In October 2014 AWS launched the AWS Directory Service to connect Windows workloads in EC2 to a directory on-premise or in the cloud. Industry pundits interpreted this as AWS launching a competitor to Microsoft's own cloud-based directory service, Azure AD. However, just over a year later in December 2015, the company also announced a managed AD service for AWS Directory Service.

The advantage of the managed AD offering is that the customer can establish one and two-way trust relationships between their AWS Directory Service for Microsoft Active Directory (Enterprise Edition) and on-premise directories, as well as between multiple Microsoft AD directories in the AWS cloud, because Microsoft AD supports all three trust relationship directions (incoming, outgoing, and two-way). In this way, the AWS Microsoft AD acts as a resource group for on-premise AD, as well as acting as a standalone AD environment for customers that don't have one on premise.

The benefit of this approach over AWS's Simple AD service, which runs on the Samba 4 Active Directory Compatible Server, is that customers continue to get all the application support they have with their on-premise AD.

With such an extensive customer base among companies large and small, it would be no surprise if AWS were to begin offering identity services for customers to access any assets in hybrid cloud environments, regardless of who is providing the assets.

Google

In a sense, Google is already a major player in identity in that it has a billion people logging into Google accounts around the globe. Beyond that, the trend toward social login/social sign-in, whereby third-party websites enable users to log in with their existing credentials from a major social network, means a lot of people are using their Google Account login details for this purpose.

But what of offering IDaaS specifically into the enterprise market as a standalone, paid-for service? Google makes no secret of the fact that it is first and foremost interested in honing its identity management skills for the vast B2C market, which is to be expected from a company with such consumer tech and services clout. This explains its research into the usability for consumers of stronger authentication methods and the usability of federated sign-in options, as well as developer tools such as Firebase Auth and SmartLock for Passwords.

Google's ambitions in the enterprise market

However, Google also harbors big ambitions in the cloud/IaaS market, and hired a stalwart of enterprise tech, VMware founder Diane Greene, to spearhead both the Google Cloud Platform (GCP, the company's emerging IaaS business) and Google Apps (the SaaS business). One senior Google executive, Urs Hölze, has gone so far as to suggest that the company's revenue from cloud services could outstrip its income from advertising by 2020.

Google is clearly seeking to mount a serious challenge to AWS and the current number two in the IaaS market, Microsoft, and identity services are an integral part of this initiative. It already offers what is calls enterprise-grade access control, permissioning, resource control, and audit trail as part of Google Cloud IAM, which provides free functionality for all GCP customers.

Partners for advanced IDaaS

However, while Google is an identity provider and offers IAM capabilities on the GCP, it refers customers requiring more advanced enterprise features to one of several partners with a greater B2E and B2B focus, such as Ping, Okta, SailPoint, or OneLogin.

A case in point is Netflix. The streaming media and video-on-demand provider has standardized on Google Apps for Work as its source of office productivity, storage, and collaboration applications for its 4,000 employees. It also uses the platform as its SSO provider for all cloud apps, including those outside of Google Apps and the Google Apps Marketplace.

Netflix required additional controls within its identity management infrastructure, beyond the ones Google provides. These additional features were in areas such as entitlements, i.e. to determine which of its employees could access which applications. The solution it came up with was to put its employees into Google Groups, then feed the list of who belongs to what Group into Ping, which carries out the enforcement of who can and cannot access what.

Where Ovum expects to see Google growing its IDaaS offerings in the short term is not in the enterprise market, but the small and medium-sized business (SMB) segment. The reason for this is that the company believes existing IDaaS specialists cannot downscale the sales costs of managing relationships with companies with headcounts in the sub-1,000 segment. For this market, therefore, paying to use Google Apps means they get an identity provider in Google.

VMware

VMware Identity Manager is an identity-as-a-service (IDaaS) offering. The solution is available as part of VMware Workspace ONE. It provides secured access to corporate applications across all devices and platforms, and single sign-on (SSO) access to cloud apps, single portal access for employee applications, and conditional access to apps based on device, network, and user.

VMware Identity Manager editions

VMware Identity Manager provides application provisioning, self-service catalog, conditional access controls and SSO for SaaS, web, cloud and native applications. It is available in two editions: Standard and Advanced.

- The Standard Edition is packaged in Horizon 6 Advanced and Enterprise and provides SSO across Horizon RDSH Apps, desktops, ThinApp, and SaaS apps, and is ready for integration into AirWatch environments.
- The Advanced Edition includes AirWatch device and registration and the AirWatch console to manage certificate-based authentication. It provides device-specific adapters for Identity Manager. VMware Identity Manager is included in the AirWatch Enterprise Mobility Management Suites and VMware Workspace.

Features and functionality

VMware Identity Manager offers the following functions and features.

- Enterprise Single Sign-On helps simplify integration with existing on-premise identity providers so organizations can aggregate SaaS and Native Mobile and Windows 10 apps into a single catalogue.
- Identity Management with Adaptive Access establishes trust between users, devices, and the hybrid cloud. It uses conditional access control facilities and leverages AirWatch device enrolment and SSO adapters.
- Self-Service App Store allows employees to search and select applications they want to subscribe to and supports automated or manual provisioning as required by the client organization.
- Enterprise-Grade Hybrid Cloud Infrastructure: Identity Manager uses the same identity management solution as vCloud Air and the vCloud Suite, facilities that are available in most advanced data center and private cloud environments.
- Directory integration and federation supports multiple AD domains, multiple forests, and different trust configurations, and offers flexible integration with existing operational environments.
- Detailed user analytics are available to help understand usage trends and capacity planning.
- Beyond app usage analytics, device analytics are supplied through AirWatch-enrolled devices to permit IT to understand the intersection of apps and devices to make intelligent decisions about capacity planning and new service development.
- Application provisioning, where once a new application is placed in the app catalog, administrators can auto-provision facilities to users by group, or enable self-service subscription.

- Conditional access policy facilities are available and can be applied by user, security group, network, and authentication strength.
- Conditional access by device distinguishes between managed and unmanaged devices to allow broad access to low-risk apps and then enforce device management with encryption and wipe controls for apps that contain sensitive data.
- Web portal facilities are available, and the Identity Manager customization tool allows organizations to personalize and configured the VMware self-service app store and launcher.

Trusted VMware facilities provide support for enterprise-grade hybrid cloud infrastructures. Identity Manager was designed for the mobile cloud world, with AirWatch-enrolled devices supporting the consumer-grade user experience.

Pre-integration with enterprise apps

VMware works with a range of enterprise SaaS vendors and makes use of the SAML standard to provide predefined integrations including support for automated user provisioning.

Hybrid deployment model

Identity Manager is built from a single multitenant code base whether deployed on-premise or in the cloud. Cloud-based and on-premise instances of Identity Manager may federate for added flexibility. Industry support for a wide range of web, virtual desktops, published applications, Windows packaged apps, and native mobile apps is available.

Oracle

Oracle has been talking about an IDaaS offering for a few years, but actually launched its Identity Cloud Service (IDCS) at its annual OpenWorld event in September 2016, with general availability announced for the following month.

Cloud-native IDaaS, not hosted OIM

IDCS was designed from the outset as a cloud service and is not the company's longstanding Oracle Identity Manager (OIM) product hosted in the cloud. That is not to say that it is the definitive article, though, as the company continues to add more features, and says it will take around a year and half for IDCS to reach the full IAM functionality level it envisages for the platform.

Oracle's new IDaaS platform is also designed to work alongside on-premise IAM technology, whether it be OIM or a product from another vendor. The company describes this scenario as leveraging customers' existing investment in IAM while adding the cloud component with IDCS, establishing trust between the two platforms and providing a single view across both for administration purposes.

This hybrid of on-premise and cloud-based identity services is still evolving. Oracle is delivering a connector from IDCS to OIM (providing the necessary trust between the two) and synchronization with the customer's on-premise Active Directory. These features are designed to enable IDCS/OIM integration out of the box, contrasting with the extensive integration work customers face if they deploy a cloud-only IDaaS service alongside an on-premise platform.

Equally, IDCS is designed to work with any existing connectors between OIM and any Web access management (WAM) technology the customer may have in place, enabling the WAM platform to continue to operate even as the Web application is moved from the customer's own data center to the cloud.

Meanwhile, there are plans for further functionality to streamline collaboration between the two environments. IDCS launches with identity management and administration, access management, and a cloud-based directory.

On the IDCS roadmap: MFA, provisioning, ID governance, and intelligence

In its next release scheduled for the January timeframe, the platform will gain multi-factor authentication(MFA) and provisioning, then later in 2017, Oracle will add identity governance and intelligence (analytics based on users' access behavior).

Philosophically, Oracle opted for an "API first", open standards-based approach to developing IDCS. The platform therefore supports SAML and OpenID Connect for authentication and authorization, SCIM for the secure, automated exchange of user identity information between identity domains, and OAuth for token-based authentication and authorization.

In addition, Oracle is on the board of the OpenID Foundation, which promotes an identity layer on top of the OAuth 2.0 protocol, which allows computing clients to verify the identity of an end user based on the authentication performed by an authorization server. As part of its membership, Oracle is a member alongside Ping Identity and Salesforce of the Fast Federation Working Group (FastFed WG), which is working to make the OpenID Connect standard more enterprise-friendly.

A zero-trust model for security microservices

In terms of the security of the platform, Oracle highlights the fact that IDCS is entirely microservices-based, with multitenancy and isolation. More specifically, it consists of 13 microservices with zero trust between them, meaning that they all need to authenticate with each other in order to interact. The company argues that this makes IDCS a prime candidate to sit at the core of a cloud-based security fabric.

Furthermore, in the first quarter of 2017 Oracle plans to roll out a series of integrations with other security platforms to enhance IDCS's overall capabilities. These will include:

- Blue Coat's Elastica Cloud Access Security Broker (CASB) platform, even though Oracle has itself recently acquired a competitor in the form of Palerra.
- enterprise mobility management (EMM) platform AirWatch.
- the user and entity behavioral analysis (UEBA) from Caspida (a vendor acquired by Splunk in mid-2015).
- Webroot for its Reputation Service.
- The leading security incident and event management (SIEM) platforms on the market.

The idea is for IDCS to run a consolidation engine, whereby it will be able to bring together risk scores from the reputation and SIEM platforms and share them with enforcement platforms such as AirWatch, Elastica, and its own Palerra CASB.

Three IDCS SKUs

IDCS will eventually be available in three SKUs:

- an Attach SKU for Oracle Public Cloud customers
- a Standard SKU for customers running cross-cloud and hybrid environments (cloud and on-premise), such as companies that want to use it for Office 365

- a Premium SKU, which will come with the Advanced Identity Governance and Identity Services, once all these features have been launched.

The Attach and Standard SKUs are available from the outset and charged via per-user annual subscriptions. There are also plans for the future development of a metered (pay-as-you-go) charging mechanism. The idea is that companies with users that connect regularly and frequently will probably prefer Standard with per-user subscriptions, while those with users who only connect occasionally will go for the metered option.

OIM is a mature product that is extremely customizable, enabling it to accommodate some of the more complex workflow requirements of large-scale IAM deployments in the high-end enterprise market, many of which are underpinned by SOA and business process management (BPM). While IDCS is scheduled to gain new functionality in upcoming releases, Oracle is waiting to see whether it will ever need to reach the level of customizability of the on-premise product.

CIAM specialists are also thriving

There is a growing need for B2C identity services

While some of the biggest names in the tech sector are moving into IDaaS, directly or obliquely, another sector that is flourishing is the subset of identity service platforms that focus specifically on the relationship between enterprises and their online customers. This B2C technology even has its own acronym, CIAM (customer identity and access management).

Ovum has seen this sector grow in recent years as interactions with customers have moved increasingly online. This has resulted in a need for the kind of security that IAM platforms have traditionally provided for employee (B2E) and business partner (B2B) scenarios. In addition, companies want to analyze their online interactions with customers for business insights, enabling them to hone their marketing more closely to individual customer needs, interests, and buying patterns.

CIAM vendors have grown up to address the requirement for this technology, and it is Ovum's suspicion that, as more and more employee interactions move online thanks to remote working and outsourcing, CIAM may well merge with mainstream IAM and IDaaS. There were early signs of this trend as the work was progressing on the Ovum Decision Matrix (ODM) report on IDaaS, which this report is designed to accompany and complement, when Ping Identity, one of the IDaaS vendors covered in the ODM, acquired CIAM specialist UNboundID in August 2016.

Janrain

Janrain is a Portland, Oregon-based company founded in 2002 by Larry Drebes, who is currently its CTO, to provide customer identity and access management, placing it squarely on the B2C side of the IAM business. Drebes himself was a founding member of the OpenID Foundation and has been a vocal advocate of the OAuth 2.0-based online authentication.

Janrain remains privately held and has so far raised $78.7m in venture funding, most recently in a $27m D Series round which closed in December 2015. The round was led by HighBar Partners, with participation from existing investors Millennium Technology Value Partners, Split Rock Partners, Epic

Ventures, Emergence Capital, RPM Ventures, and DFJ Frontier. Janrain's enterprise customer base includes Pfizer, Samsung, Whole Foods, Fox News, Philips, Marvel, and Dr Pepper.

Delivering CIAM from a cloud-based platform, Janrain divides its offerings into six distinct "products":

- **Social login**, which enables website and mobile users to register and log in to a company's site with their existing social network identities from Facebook, Google+, Twitter, LinkedIn, and some 30 other providers.
- **Registration**, which gives companies the online tools to acquire and recognize customers across all their web and mobile properties without building or maintaining their own registration platform. Registration and data collection forms, profile pages, account creation flows, password management, and field validation are available out of the box and are customizable to meet company-specific needs. The solution also supports traditional registration and works in tandem with social login.
- **Profile data storage**, which enables companies to collect, store, and manage demographic, psychographic, and behavioral customer profile data in the Janrain cloud, in an automated way. Janrain provides a customer profile database and the tools companies need to access and manage the data. It is designed to facilitate the integration of customer data with the marketing applications companies are using, and to scale to accommodate high volumes
- **Single sign-on**, where customers can register or log in once and navigate across a company's multiple websites without needing to log in again. SSO is designed to create a better customer experience and reduce abandonment by keeping customers logged in across as many sites as required.
- **Engagement**, which provides a service that promotes real-time conversations, drives customer acquisition, and makes it easy for customers to interact with a company's site content and share with their friends. It analyzes the results for customers participating in commenting, live chat, voting, and rating and reviews, helping companies determine which activities drive the most site registrations. It also derives real-time analytics on social media activities to give marketers insight into customer behaviors on social media.
- **Customer insights**, which provides dashboards to visualize and segment customer profile data based on any demographic, psychographic, or behavioral attributes stored within Janrain, enabling companies to improve conversions and make better decisions with insights into social login trends, registration events, activities, and social sharing metrics.

All these modules within the overall Janrain service were built with the B2C market in mind, and it is there that Ovum sees the company challenging the IAM and IDaaS players that come from the B2E side of the business.

However, as online interactions with customers become far more prevalent than face-to-face meetings with them, and as more and more employees and partners start to operate like customers, in that most of their interactions with a company are online rather than in the office, B2C could become the tail that wags the dog in IAM, which is why it is worth keeping an eye on Janrain.

Gigya

Gigya was founded in 2006 by Rooly Eliezerov (its current president), chief strategy officer Eyal Magen, and CTO Eran Kutner. It is headquartered in Mountain View, California and remains privately held, having so far raised a total of $104m. Its most recent funding round was for $35m in November

2014, when Intel Capital was the leader. The company has 325 employees and some 700 enterprise customers, including NBC, Forbes, AutoTrader, Dell, PacSun, Tommy Hilfiger, and Barneys New York.

Gigya offers three levels of its customer identity management (CIM) service: Identity, Identity Plus, and Identity Enterprise.

Identity comprises:

- Social login plugin, designed to reduce so-called "login friction" by enabling customers to use their existing credentials from social networking sites, while at the same time providing companies with permission-based access to the customers' first-party data on those sites.
- Profile management.
- Passwordless mobile authentication.
- Roles and permissions.
- Analytics (a series of reports on matters such as new users, demographics, and referred traffic).
- Customer insights, which provides the ability to visualize the demographic data of any user who connects with a company's brand, including age, gender, relationship status, and location.
- Identity access for managing high volumes of user records and viewing data on any customer within a database on a dashboard, enabling search by email, name, user ID and so on to view users' profile details and edit site-specific data.
- Identity compliance, enabling compliance with privacy legislation, with features such as automatic account deletion, as well as keeping user data fresh with automatic record updates as users change their Facebook entries on their locations, relationship statuses, and interests.

Identity Plus has all of the above, as well as:

- Registration-as-a-service.
- Customer Insights Plus to gain a deeper understanding of users, viewing their Facebook Likes, favorite brands, and so on.
- Progressive and conditional profiling to capture additional identity data over time as customer relationships develop, and optimizing registrations with conditional workflows that automatically trigger form fields based on inputs to previous fields or pre-existing data about a user.

Identity Enterprise adds:

- A data store feature for user-related data, enabling only what needs to be instantly accessible to stay in profile management.
- Federation.
- Two-factor and risk-based authentication.
- Signals to define and track custom, on-site activities such as purchase behaviors and ad clicks.
- Auditing for monitoring user-level privileges and permissions within the Gigya administrative console.
- Single sign-on

Gigya's focus is clearly on the B2C side of the IAM business, where there is evidently huge demand as companies conduct more and more business online and need increasingly sophisticated ways of managing, segmenting, and analyzing the data they are amassing on their customers. Here again, though, there is an argument that such cloud-based technology for managing customer interactions might ultimately subsume the B2E and B2B variants of IAM.

Appendix

Further reading

Ping UnboundID acquisition shows B2C is the future of identity, IT0022-000781 (September 2016)

On the Radar: Gigya, IT0020-000156 (September 2015)

On the Radar: UnboundID, IT012-000055 (January 2012)

"*UnboundID aims to move up the identity value chain,*" IT012-000061 (August 2012)

Author

Rik Turner, Senior Analyst, Infrastructure Solutions

rik.turner@ovum.com

Andrew Kellett, Principal Analyst, Infrastructure Solutions

andrew.kellett@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo

Ovum
TMT intelligence | informa

Ovum Decision Matrix: Selecting an Identity-as-a-Service (IDaaS) Solution, 2016–17

Publication Date: 07 Dec 2016 | Product code: IT0022-000836

Andrew Kellett

Summary

Catalyst

Identity-as-a-service (IDaaS) is the cloud alternative to maintaining identity and access management (IAM) products on-premise. Fully featured IDaaS offers authentication, access control, single sign-on (SSO), provisioning and password management, infrastructure and directory management, reporting, alerting, and monitoring services, and is hosted, managed, and delivered as a cloud-based service.

IDaaS is relevant to a wide range of organizations, including first-time clients that see it as providing an identity management opportunity they can benefit from and afford. It is relevant to existing IAM users that want a new way of working with identity management that doesn't involve owning and maintaining the on-premise infrastructure. Organizations that need to extend their IAM coverage to the cloud would also benefit from a hybrid approach to the IDaaS service delivery model. Similarly, companies that already have a significant investment in an IAM platform might take advantage of an IDaaS service, say for a new business unit, to avoid the overhead involved in adding an entirely new group of people into their on-premise identity infrastructure.

Ovum view

IDaaS is relevant to public and private sector organizations that are prepared to allow their IAM services to be managed and maintained from the cloud, and are willing to work with a third-party service provider. Data protection regulations, risk, and security concerns are commonly cited as reasons for not going ahead, but a growing number of CIOs and CISOs consider the business risk to be acceptable and are building their IDaaS strategies.

Traditional approaches to IAM continue to have their place, but are often seen as overly complex and costly, leaving clear ground for the providers of lightweight IDaaS to push forward with the efficiencies, flexibilities, and cost savings that are said to be an inherent part of the IDaaS approach.

However, not all IDaaS service providers can deliver all the expected components of identity management. Some are interested only in enabling access to cloud-based applications with their technology, and are prepared to leave the enterprise heavy lifting to technology partners or competitors that can deal with a hybrid mix of on-premise products and cloud-based services.

The cloud-only approach misses the important point about how next-generation identity management needs to evolve. It needs to be capable of providing an integrated strategy for the management of identity across business-to-business (B2B), business-to-employee (B2E), and business-to-consumer (B2C) operations, whether these services are delivered on premise, from the cloud, or federated with a trusted business partner.

A more sustainable approach, and a better way to consider IDaaS, is to recognize that it can and should offer the opportunity to streamline identity and access management and provide an enterprise-wide approach that deals with on-premise as well as cloud-based relationships. IDaaS technology is evolving but is still not mature. Nevertheless, the number of identity management vendors that now offer fully featured IDaaS is growing, as IDaaS specialists that started out delivering cloud-only solutions clash with early-to-market IAM platform vendors that see IDaaS as a natural extension to their core IAM portfolios.,

Therefore, to maintain and build on its early successes, the IDaaS community must begin to offer a balanced package of identity services that match the enterprise requirement of seamlessly and securely managing access to both cloud and on-premise systems.

Key findings

- The IDaaS market is relatively immature and continues to be led by the original group of specialist providers.
- IDaaS provides a mainly cloud and services-led approach to identity management using a hosted model to deliver core identity and access management services.
- IDaaS can offer a realistic, cloud-based alternative to maintaining IAM products on premise.
- A services-led approach to identity management is relevant to both public and private sector organizations and can meet the needs of most industry verticals.
- There were functional shortfalls in some first-generation IDaaS solutions that made them unfit for enterprise clients.
- Mainstream IAM providers were slow to recognize the need for an IDaaS strategy. Most are still playing catchup, and some will need to make acquisitions to get to the first rung on the ladder.
- Leading IDaaS providers offer a hybrid mix of identity management services that can support enterprise-wide operations.

Vendor solution selection

Inclusion criteria

IDaaS technology has to move on from a position of specialization where cloud usage and cloud service delivery were intrinsically connected. There are relatively few cloud-only businesses, and the majority of potential clients will have already deployed IAM solutions and have the supporting infrastructure services in place.

Some will be looking for a replacement strategy, and a few will be first-time users who see real possibilities in IDaaS. Most will be looking for a mixed, hybrid approach that brings together their on-premise and cloud-based operations to deliver an integrated set of identity management products and services. To achieve all these objectives requires IDaaS services to support mainstream B2E, B2B, and B2C usage and a full range of business and user demands. This includes most of the measures and facilities listed below:

- IDaaS technology needs to support multiple use cases, including cloud-only operations and a hybrid mix of cloud and on-premises systems, and must be capable of replacing or working alongside legacy, platform-based IAM tools.
- It needs the ability to support major client relationships including business-to-business (B2B), business-to-employee (B2E), and business-to-consumer (B2C), as well as machine-to-machine and IoT interactions.
- It should deliver core identity management services that include authentication, access controls, SSO, federated identity management, provisioning and de-provisioning services,

self-service registration and password management, directory integration and management, reporting, alerting and monitoring, and identity governance.

- It should have the ability to operate alongside and integrate with mainstream third-party IAM systems.

Exclusion criteria

There continue to be IDaaS specialists that focus only on particular disciplines, such as authentication-as-a-service, customer-facing identity management, or that only support cloud-based operations. Their coverage would be considered too narrow for this report. However, IDaaS continues to be positioned as an emerging business- and technology-focused approach to identity management and as such, some of the vendors included in this report cannot cover all areas of identity management without assistance from a technology partner. Vendors have been excluded if they:

- Only offer a narrow range of IDaaS services.
- Do not have the capacity or scale to deal with medium-to-large enterprise as well as small-to-medium business requirements.
- Do not have the facilities in place to work alongside mainstream technology partners in the identity management space.
- Do not have the maturity, revenues, or market presence to compete with the leading IDaaS providers.

Methodology

Technology/service assessment

In this assessment dimension, Ovum analysts have identified a series of features and functions that provide differentiation between the leading solutions in the marketplace. The criteria groups identified for IDaaS are as follows:

- IDaaS service delivery addresses service delivery capabilities for cloud, web, and on-premise requirements, and also covers key operational environments that need to be supported (B2B, B2E, B2C, M2M, and IoT), and the delivery of core identity management services.
- Authentication drills down into the capabilities supported, such as, for example, how one-time passwords (OTPs) can be generated and the approaches delivered, and the business and social mediums available.
- Single sign-on (SSO) covers the range of SSO facilities supported, its on-premise and cloud interoperability and threat protection capabilities, and its security controls.
- Federation and the range of facilities available are used to manage relationships between company and business partner networks, including the federation of SSO interactions.
- Provisioning facilities are provided and the services supported include de-provisioning and associated reporting and alerting services.
- Directory management facilities provide support for key directories that fall within the IDaaS and IAM criteria, along with associated requirements for directory synchronization.
- Reporting, alerting, and monitoring requirements and the levels of service that need to be maintained are considered.

- Management and infrastructure covers elements such as the range of applications supported with pre-written APIs, key industry standards supported, and the third-party IAM systems each IDaaS service can work alongside and integrate with.

Execution

In this dimension, Ovum analysts review the capabilities of the solution around the following key areas:

- Maturity: the stage that the product/service has achieved in the IDaaS maturity lifecycle is assessed here as it relates to the overall technology/service area.
- Interoperability and innovation: we assess how easily and how well the offerings and their forward-looking features are made available to allow them to be integrated within an organization's operational systems and services.
- Deployment: refers to a combination of usage and support elements that cover various deployment issues, including services, support, and update/release requirements.
- Scalability: points of referenceable achievement are used to show the scalability of the solution across small, medium, and large operational environments.
- Enterprise fit: covers the alignment of the solution to business requirements and the potential cost overheads identified.

Market impact

The global market impact of a solution is assessed in this dimension. Market Impact is measured across four categories:

- Revenues and growth: each solution's IDaaS revenues are identified and measured alongside the revenue growth that has been achieved over the last 12 months.
- Geographic penetration: existing revenues across four major trading regions: North America, South America (LATAM), Europe, the Middle East, and Africa (EMEA), and Asia-Pacific, are taken into account.
- Vertical penetration: this is determined by each solution's overall presence in the following industry verticals: banking, energy and utilities, education, investment services, healthcare, insurance, legal services, life sciences and pharmaceuticals, manufacturing, media and entertainment, professional services, public sector, retail, wholesale, and distribution, and telecoms, and travel transportation and logistics.
- Size-band coverage: this determines the presence each vendor has across small, medium, and large business operations.

Ovum ratings

- **Leaders:** This category represents the leading solutions that we believe are worthy of a place on most technology selection shortlists. Each vendor has established a commanding market position with a product/service that is widely accepted as best of breed.
- **Challengers:** Each solution in this category has a good market positioning and offers competitive functionality and good price-performance proposition, and should be considered as part of the technology selection.

Market and solution analysis

Ovum Decision Matrix: Identity-as-a-Service (IDaaS) 2016–17

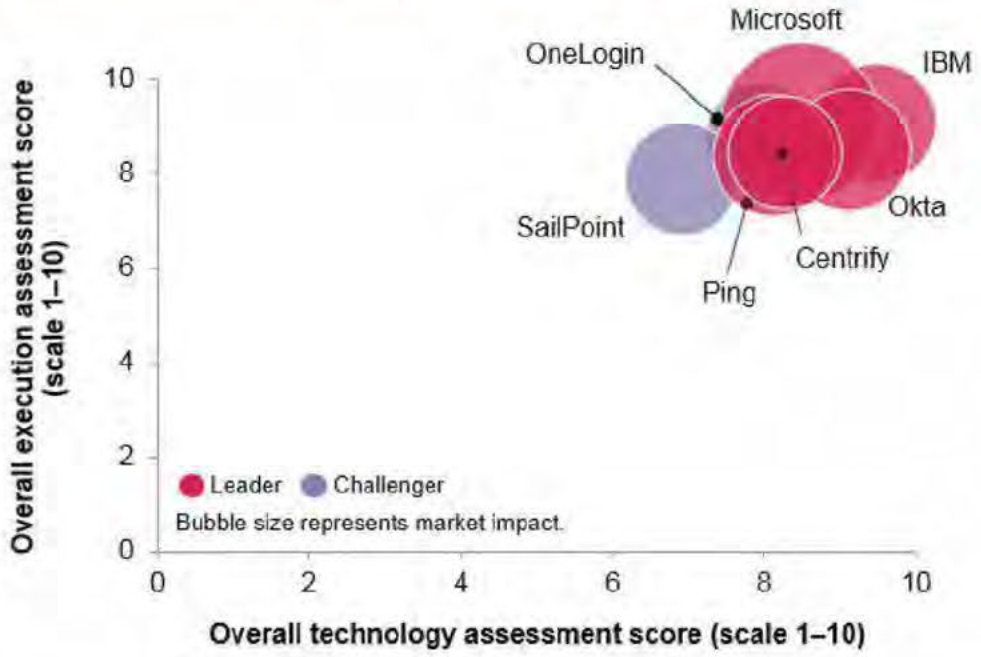
Identity-as-a-service (IDaaS) offers a viable alternative to traditional on-premise identity and access management (IAM) platforms. IDaaS efficiencies and cost-savings are relevant to most business operations, but not necessarily as a complete replacement for existing technology, because hybrid IDaaS and core IAM platforms can be deployed and coexist to the benefit of organizations and their users.

The emerging IDaaS market consists of two main groups: next-generation identity management providers such as Centrify, Okta, OneLogin, and Ping that came into being to deliver identity-based services from the cloud, and established IAM platform vendors, including IBM, Microsoft, and SailPoint, that have already gone some way toward developing their IDaaS strategies.

For the cloud-driven originators of IDaaS, the starting position was to deliver secure access to cloud-based services. The leaders in this market have now gone on to develop enterprise delivery strategies and services that support the hybrid identity management requirements of both on-premises systems and cloud-based applications.

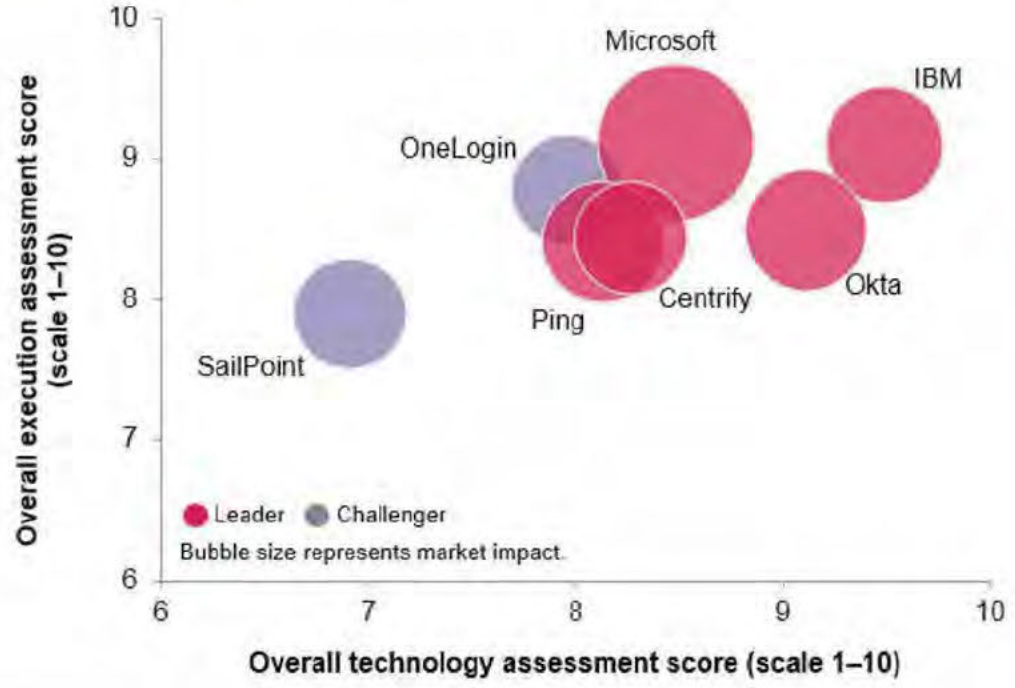
Established IAM platform vendors see IDaaS either as an opportunity to build new services and address new markets, or as a problem that threatens the status quo. Some have made an effective response and are developing technology solutions that operate alongside their on-premise facilities, either as an extension to the existing IAM infrastructure or as free-standing alternatives. Others were late to market, have more technology on their roadmap than in production, and will be playing catch-up for some considerable time.

Figure 1: Ovum Decision Matrix: Identity-as-a-Service (IDaaS) 2016–17



Source: Ovum

Figure 2: Expanded view of Ovum Decision Matrix: IDaaS 2016–17



Source: Ovum

Table 1: Ovum Decision Matrix: IDaaS 2016–17

Market leaders	Market challengers
Centrify	OneLogin
IBM	SailPoint
Microsoft	
Okta	
Ping	

Source: Ovum

Market leaders: vendor solutions

The market leaders group consists of an eclectic mix of cloud-focused identity management vendors: Centrify, Okta, and Ping. It also includes the established IAM platform provider IBM whose IDaaS credentials were established following the acquisition of Lighthouse and its IDaaS technology in 2014, plus Microsoft, which retains traditional IAM coverage but has a stronger and more natural sense of presence in the IDaaS community.

Centrify delivers its portfolio of identity management products and services from the cloud, and from the company's inception has maintained a cloud-first service delivery strategy. Its IDaaS approach covers its core identity management and its privilege management portfolios. For both products,

Centrify provides a multi-tenant, cloud-based, software-as-a-service (SaaS) solution. It offers context-aware and adaptive multifactor authentication, enterprise and federated SSO, provisioning and password management, and cloud and web-centric access control facilities.

IBM launched its IDaaS offering two years ago with the acquisition of the Lighthouse Security Group, and its Cloud Identity Service (CIS) continues to evolve to meet future identity management and business protection requirements. IBM CIS is now an integrated component of the company's IAM portfolio and supports its complete range of identity management, web access management, and federated identity management services.

Microsoft's IDaaS facilities are delivered using the company's Azure Active Directory products. As a pure IDaaS solution, Azure Active Directory provides SSO access to the cloud-based applications organizations choose to deploy. For hybrid environments, it delivers secure remote access to on-premise and web-based applications. Microsoft also provides integration with on-premise directories and connectors to synchronize with their cloud-based equivalents.

Okta is a cloud-native provider of IAM services. Since the company's foundation in 2009, all its identity-based services have been delivered from the cloud. It offers a full range of IDaaS products and services including directory controls and management, SSO, user and device lifecycle management that includes provisioning services, adaptive and multi-factor authentication (MFA), enterprise mobility management, and API access management.

Ping offers a comprehensive suite of IDaaS products that deliver a seamless approach to identity management across business and consumer environments. Its identity-as-a-service capabilities provide secure access to all supported applications, and federated management extends control so that organizations can manage inter-company relationships and provide secure access to shared applications, resources, and services. Ovum is particularly encouraged by the recent expansion of its consumer identity capabilities with the acquisition of UnboundID.

Market challengers: vendor solutions

As was the case for the leaders group, the challengers consist of an IDaaS specialist (OneLogin) and a vendor that straddles the divide between core IAM platform services and a next-generation approach to IDaaS (SailPoint).

OneLogin has from its inception been a cloud-based IAM vendor, with identity management delivered using an IDaaS approach. The company started out providing identity-based access to cloud applications for SMEs, but has since expanded into a full-fledged IDaaS platform, and its customer base now also includes large enterprises. It supports a full range of business-to-employee (B2E) and business-to-business (B2B) identity services and is looking to add more business-to-consumer (B2C) features.

SailPoint is an established provider of IAM technology. It started out with an on-premise software product in the second half of the last decade, and in 2013 added IdentityNow a cloud-based service product. IdentityNow offers a full IAM service in the cloud, with user provisioning, SSO (including support for federated SSO), password management, access certification, and data governance features.

Emerging vendors

Table 2: Emerging vendors: IDaaS 2016–2017

Amazon Web Services (AWS)	Janrain
CA Technologies	Oracle
Gigya	Salesforce.com (SFDC)
Google	VMware

Source: Ovum

The emerging vendors section looks at companies that did not make it onto the list of those subjected to our full examination for the vendor comparison process, but that we nonetheless consider worthy of our readers' attention. For example, two IAM incumbents, CA and Oracle, are moving into the IDaaS market, but were not quite ready to submit to the full comparison process. Smaller, dedicated IDaaS players that focus primarily on the business-to-consumer side of the market and describe what they provide as customer identity and access management (Janrain) or customer identity management (Gigya) are included here. The final group includes major industry players that are neither traditional IAM vendors nor IDaaS startups, but which by virtue of their clout elsewhere in the hi-tech sector are well placed to move into cloud-based identity management. These include Amazon Web Services, Salesforce.com, Google, and VMware.

New entrants

CA Technologies recognizes that a growing number of its business clients require full-featured IAM services that can be delivered from the cloud. Its new IDaaS facilities, which at the time of publication of this report were being released, will offer authentication, provisioning, and entitlements management, SSO services, and access controls that support the hybrid mix of on-premise and cloud-based services that most organizations have deployed.

Oracle has been looking toward the development of an IDaaS offering for some time, but didn't actually launch its Identity Cloud Service (IDCS) until September 2016. IDCS was designed specifically as a cloud service and is an extension of the company's Oracle Identity Manager (OIM) product. It isn't, however, the finished article, and the company will continue to add features over the next 18 months. IDCS is designed to work independently and alongside on-premise IAM technology from Oracle and third-party IAM vendors.

Smaller, dedicated B2C players

Gigya offers three levels of its Customer Identity Management (CIM) service, positioning it strongly on the B2C side of IAM. Its basic identity service comprises social login/plugin facilities; profile management; password-less mobile authentication; roles and permissions; analytics; customer insights; identity access for managing high volumes of user records; and identity compliance with support for privacy legislation. Identity Plus adds to the above with registration-as-a-service; customer insights plus; and progressive and conditional profiling. Identity Enterprise then adds a data storage feature for user-related data; federation; two-factor and risk-based authentication; signals to define and track on-site activities; auditing; and SSO.

Janrain provides customer identity and access management (CIAM), positioning it on the B2C side of IAM. Delivering IDaaS-based CIAM technology from the cloud, Janrain offers six distinct products: Social Login, which enables website and mobile users to log into a company's site; Registration, which provides the tools to acquire customers across all web and mobile properties; Profile Data Storage, which enables companies to collect, store, and manage data; SSO for single customer registration and login; Engagement to promote real-time conversations; and Customer Insights, which provides dashboards to visualize and segment customer data.

Major industry players

Amazon Web Services (AWS) is the market leader in cloud infrastructure services, with 10 times more computing capacity than the next 14 cloud providers combined. In 2010, the company added IAM services to help its expanding customer base manage secure employee access to AWS instances. AWS, with its IDaaS approach to identity management, enables customers to manage access to compute, storage, database, and application services in the AWS Cloud.

Google is an established player in identity management, insofar as it has 1 billion people logging into Google accounts around the globe supported by the use of social login/social sign-in facilities. From an enterprise perspective, its IDaaS credentials are less well established, but are specifically focused on the vast business-to-consumer (B2C) market. This also explains its research into and strong interest in the usability for consumers of stronger authentication methods, and the usability of federated sign-in options.

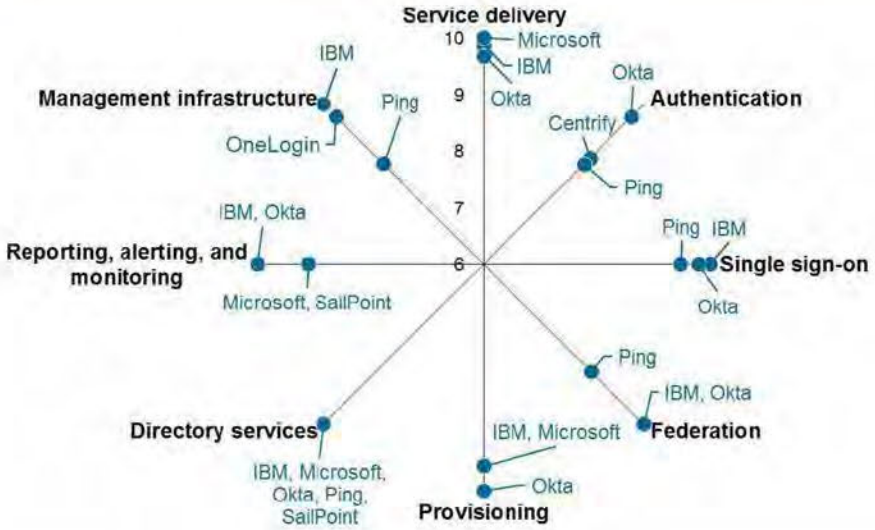
Salesforce.com (SFDC) has been in the IDaaS market since October 2013, when it launched the Salesforce Identity service. Its services are targeted at all the major use cases of identity management including business-to-employee (B2E), business-to-business (B2B), and business-to-consumer (B2C). Its plan is to enable CIOs to deliver a simple, productive, and customized user experience across all available web, mobile, and on-premise applications.

VMware's VMware Identity Manager delivers the company's identity-as-a-service (IDaaS) offering. It is available as part of VMware Workspace ONE and provides secure access to corporate applications across all supported devices and platforms. It delivers SSO access to the cloud, as well as a range of web and native applications; portal access to employee applications; and conditional access to business applications based on the device, network, and user. It also offers application provisioning and self-service catalog facilities, and AirWatch technology adds to the company's IDaaS proposition and brings mobility and mobile access into the equation.

Market leaders

Market leaders: technology

Figure 3: Ovum Decision Matrix: Identity-as-a-Service (IDaaS) 2016–17, Market leaders – technology



Source: Ovum

Centrify provides IDaaS technology services for IAM and PAM environments, and while its multi-tenant, B2B, B2E, and B2C approach to IDaaS saw it score well across most technology areas, it only made the market leader grid for authentication where it appeared alongside Okta and Ping.

IBM CIS addresses serviceability with a mobile-first approach that supports ongoing change management requirements in fast-moving business environments. Its IDaaS solution includes the same depth of identity management, web access control, and federation that are found in the on-premise platform version of its IAM technology. As a result, IBM was a consistently strong performer across most of the listed IDaaS technology components and appeared on the leader board for service delivery, SSO, federation, provisioning, directory services, reporting/alerting/monitoring, and management infrastructure.

Microsoft with its Azure Active Directory technology provides portal-based access to services and applications for all user types and was successful on the leader table across half of the major technology components, including service delivery, provisioning, directory services, and reporting/alerting/monitoring.

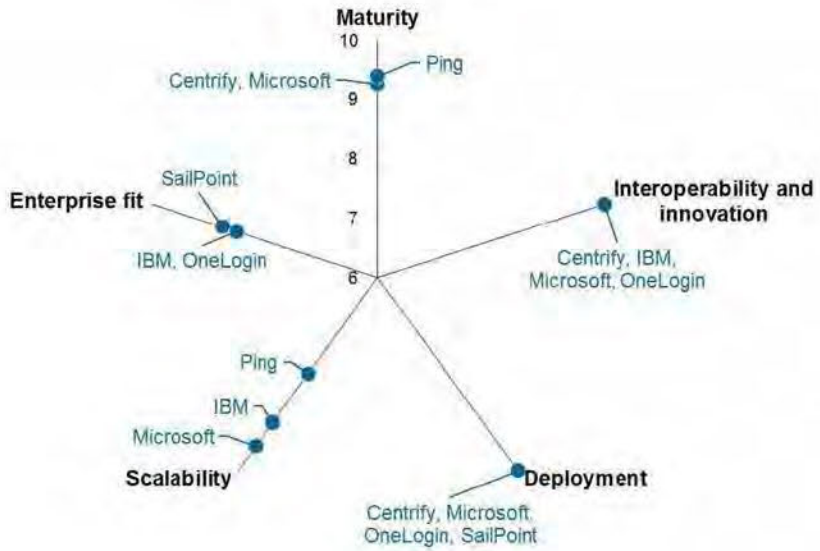
Okta provides a full IDaaS platform offering and continues to add essential new functionality. This approach shows up well in the technology leaders section, with Okta appearing in the top group in every area apart from management infrastructure. Ping, which has similar cloud-based origins, performed almost as well, with leader group appearances for authentication, SSO, federation, directory services, and management infrastructure.

OneLogin has an established reputation for covering all the basic components of an IAM platform when delivered from the cloud, particularly in the areas of provisioning, SSO, authentication, and federation. It scored well in all these areas, but was just outside the leading positions and only featured in the top group for management infrastructure.

SailPoint, which brings a decade of solid performance in the IAM market to the IDaaS arena, is primarily seen as an enterprise player, but it only made the top three for directory services and reporting/alerting/monitoring.

Market leaders: execution

Figure 4: Ovum Decision Matrix: Identity-as-a-Service (IDaaS) 2016–17, Market leaders – execution



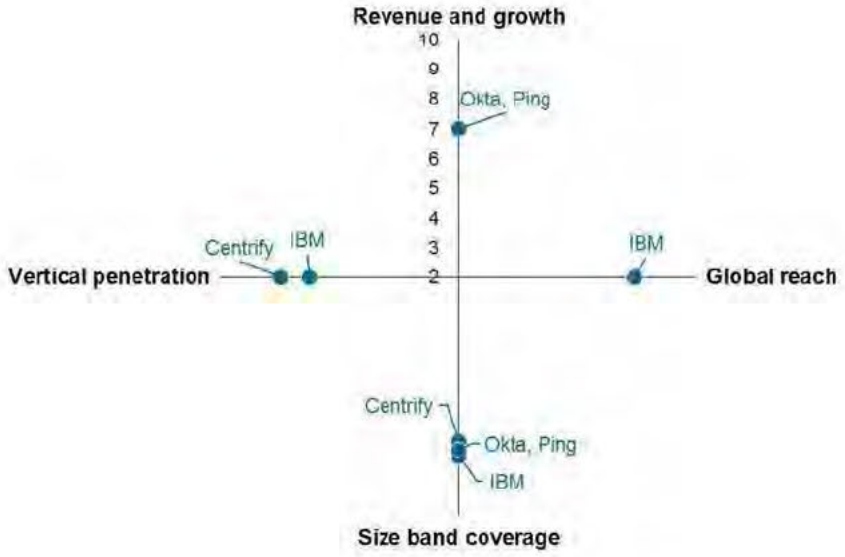
Source: Ovum

The market execution section focused on the key areas of product and services maturity, interoperability and innovation, deployment of service, scalability, and enterprise fit. Not surprisingly, most of the leaderboard (top three) positions in these key areas for business were taken up by the IDaaS market leaders. Microsoft led the way, appearing in four out of the five sections (maturity, interoperability and innovation, deployment, and scalability). Centrify (maturity, interoperability and innovation, and deployment), IBM (interoperability and innovation, scalability, and enterprise fit), and OneLogin (interoperability and innovation, deployment, and enterprise fit) featured as leaders in three out of the five categories.

The remaining leadership positions were shared between Ping (maturity and scalability) and SailPoint (deployment and enterprise fit).

Market leaders: market impact

Figure 5: Ovum Decision Matrix: Identity-as-a-Service 2016–17, Market leaders – market impact



Source: Ovum

The main areas of focus within the market impact section were on revenue and growth, global reach, size band coverage, and vertical penetration. All of these are extremely relevant measures of success in emerging markets such as IDaaS, where take-up and use in the business community is growing but remains at the early-adopter stage of the business usage lifecycle.

Combining revenue and growth provided some interesting results, with most vendors able to report year-on-year growth figures that exceeded 25% over the last financial year. However, in most cases, growth was measured against previously modest sales figures. Therefore, for all but the market leaders, performance levels were held back by the actual revenues involved. The two vendors that clearly outperformed the rest were the long-established IDaaS vendors Okta and Ping, both of which were able to maintain high levels of growth alongside revenue figures well above market average.

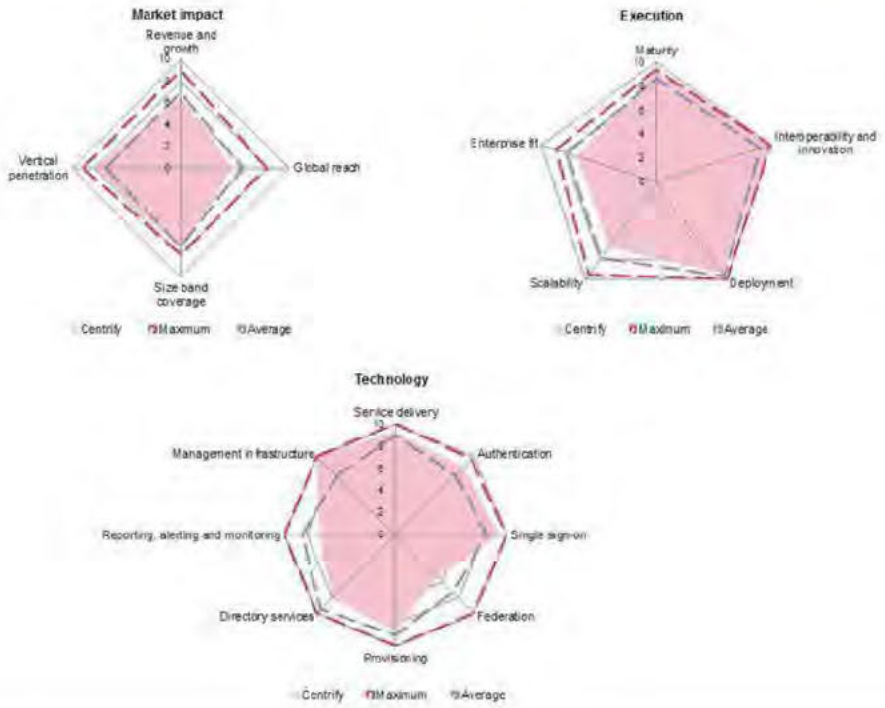
Global reach was also an area where most struggled to establish a strong position. Only IBM was able to confirm an established and even split of sales across the four key regional markets of North America, South America, EMEA, and Asia-Pacific. Others appeared to have a strong US marketing bias and some had very little presence in other areas.

Size band coverage provided a stronger position for a fair proportion of the vendors, with Centrify, IBM, Okta, and Ping having a good split of clients across small, medium, and large enterprise markets. Two of these three vendors, Centrify and IBM, were also able to quantify their vertical penetration position across the key industry verticals specified for the report.

Vendor analysis

Centrify (Ovum recommendation: leader)

Figure 6: Centrify radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

Security is at the center of the Centrify approach to IAM

Centrify's IDaaS architecture has been built from the ground up to address the protection requirements of all its users, with the emphasis on maintaining secure access to their data. Its secure cloud-based infrastructure doesn't expose, store, or log users' Active Directory (AD) credentials, or unnecessarily replicate any AD or customer data to support its operations.

Centrify IDaaS delivers identity and privileged identity services

Centrify provides two main products for the IDaaS market. Its Identity Service offers a full-featured SaaS approach and is aligned with the company's well-respected EMM mobile and Mac management solution. Its Privilege Service also offers a SaaS solution that manages shared and privileged account management in the PAM environment.

Portal-based facilities simplify access for business users

A customizable and cloud-based user portal provides one-click access to web and SaaS applications for business users with B2E relationships. It provides user self-service for mobile devices, improves visibility over users' AD account attributes, delivers activity reports detailing personal usage to help

identify suspicious activities, and provides self-service account management to deal with locked accounts and password resets.

B2B and B2C relationship management extends coverage to business partners and social environments

B2B federation capabilities allow business partners to federate their own identity provision with Centrify, enabling Centrify's clients to share approved applications and resources without the need to manage partner identities. B2C services support social login and self-service sign-up from key providers such as Facebook, Google, LinkedIn, and Microsoft.

Weaknesses

Centrify doesn't have a strong enough position in IoT and M2M management

Centrify has built its functionality within the IDaaS space to extend from its core B2E position, and it now also supports B2B and B2C relationships. However, progress in the important areas of Internet of Things (IoT) and machine-to-machine (M2M) management hasn't received a similar boost, and this appears to be especially true on the privilege side.

Opportunities

Up to a quarter of all business data interacts directly between originating device and SaaS-based applications

As growing volumes of data flow outside traditional on-premise network infrastructures, a more inclusive approach to user and data protection is needed. This by implication puts greater emphasis on the need for identity-based controls that can provide secure and measurable access to all information resources. Specifically, this would include service providers such as Centrify that can deliver safe access over public networks to commonly used cloud services such as Microsoft Office 365, Amazon Web Services, Google, Salesforce.com, and Box.

Mobile and cloud are the key drivers for the next generation of customer-facing IAM services

Mobility and cloud (mobile device and access channel of choice) are important usability drivers, especially in the consumer space. For this sector in particular, mobile devices are also increasingly used to support and deliver MFA. Scale and flexibility are the key issues when organizations select an IDaaS provider capable of dealing with their consumer-facing IAM requirements and the fast-moving nature of the apps that support these services.

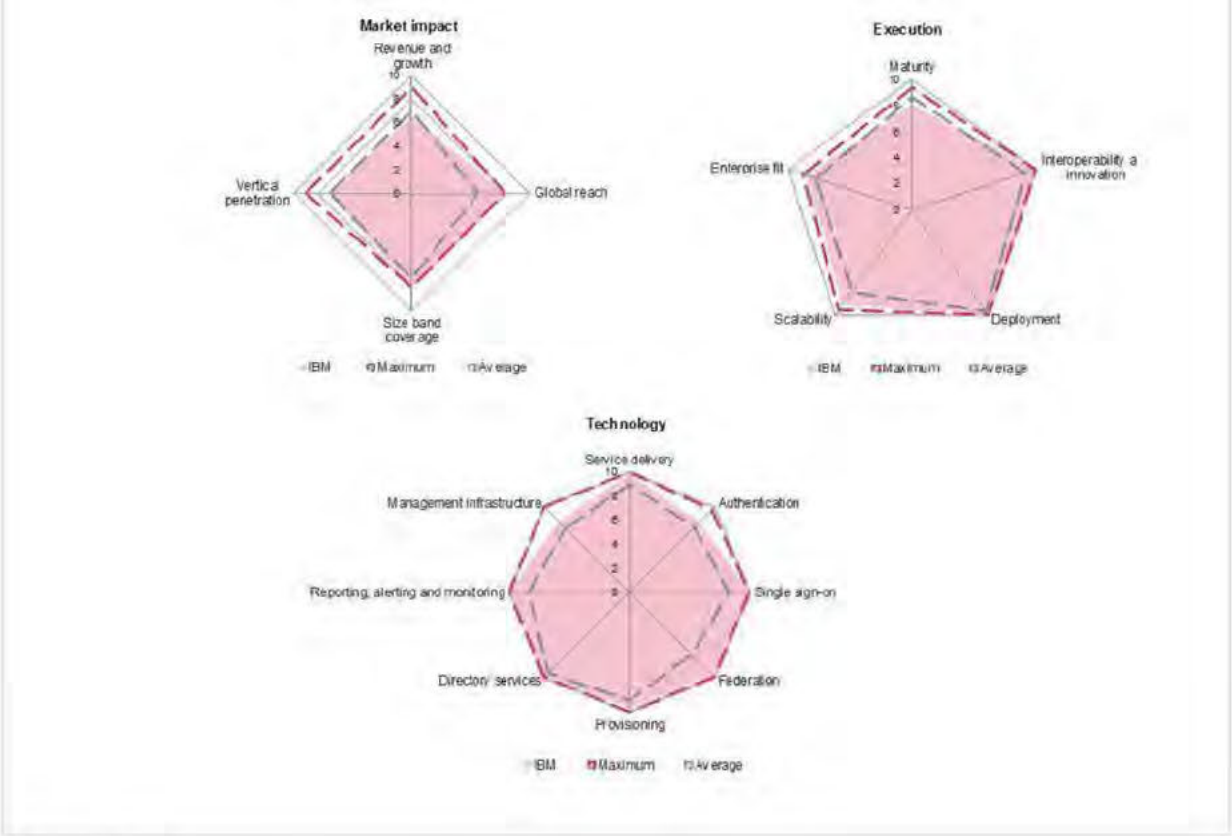
Threats

Not all organizations are ready for identity to be delivered from the cloud

Centrify leads the market in its strategy to deliver everything within the identity and privileged account management arena from the cloud. While the enterprise direction of travel continues to be toward the delivery of identity from the cloud, a significant number of organizations still see cloud-based identity and privilege management as a step too far.

IBM (Ovum recommendation: leader)

Figure 7: IBM radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

IBM Cloud Identity Service deals with cloud, on-premise, and the hybrid mix

IBM Cloud Identity Service is targeted at organizations that want to deploy IAM as a complete set of IDaaS cloud-driven facilities. It also has the enterprise functionality and alignment capabilities to operate in combination with IBM's existing on-premise infrastructure, extend operations out to the cloud, and deliver hybrid enterprise requirements.

An inclusive set of identity and access management services are on offer

IBM Cloud Identity Service identity management components offer enterprise scale provisioning and de-provisioning, self-service management, governance, user monitoring, analytics, and security intelligence. Web access management provides multi-factor, risk-based, and step-up authentication as well as auditing and user authorization services, and its federation services deliver federated SSO and federated provisioning services.

Global and local SoftLayer datacenter platforms support the IDaaS operation

SoftLayer infrastructure-as-a-service (IaaS) datacenter platforms provide global and local coverage for the service. They offer broad geographic coverage and availability that help clients address

security and data privacy regulations, including industry and local requirements, and assist in overall performance by reducing local latency.

Weaknesses

IBM needs to grow IDaaS sales beyond the enterprise

The natural comfort zone for IBM IDaaS is large enterprise, including its own IAM customer base. It needs to extend to include a wider variety of SaaS and PaaS buyers, including SMBs, line-of-business decision-makers, and developers, and in what is becoming a highly competitive sector of IAM, success will also be measured by take-up from beyond the enterprise.

Opportunities

IBM's established expertise in the security and IAM markets helps deliver its IDaaS services

The delivery of IDaaS services needs the support of industry experts. IBM's long and established expertise in the security and identity management markets puts it in a strong position to develop and support the types of IDaaS services that will address the next-generation identity protection and usability demands of enterprise clients.

There are future convergence opportunities on the IDaaS roadmap

IBM already has a full stack of IAM services available. However, further integration and convergence opportunities have been identified for its roadmap strategy, including integration with QRadar intelligence services, convergence with IBM's Fiberlink MaaS360 mobile device management (MDM) to deal with mobile access, and shared information flows with cloud access security broker (CASB) technologies, including IBM's own Cloud Security Enforcer product.

Threats

Agility and the need to support cloud and hybrid services can add unwanted complexity

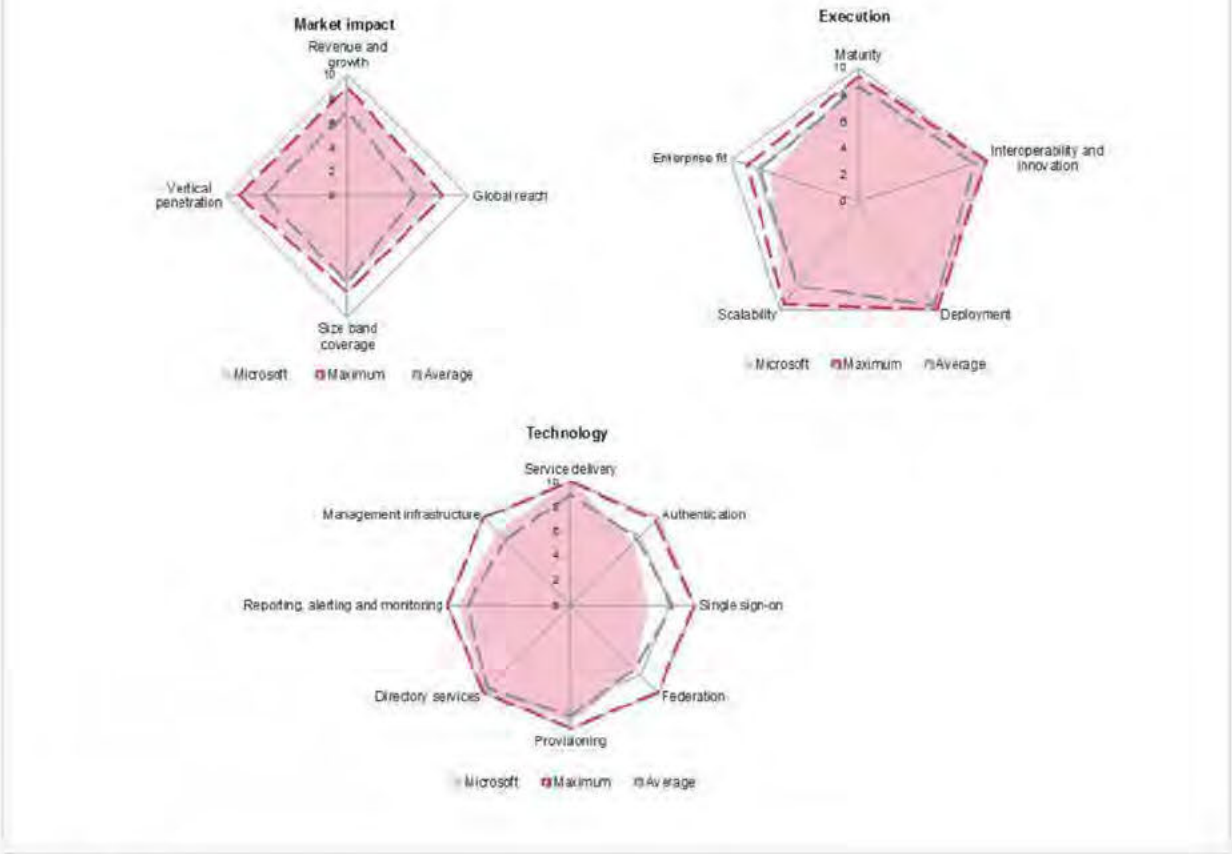
The IDaaS message from IBM is one of technology completeness alongside the ability to support an often complex mix of hybrid enterprise deployments. Others are going for the simplicity of use and deployment message, which during new business competitions can sound like a more compelling message. Increased focus is needed on how IBM will compete with the newer IDaaS players and their lightweight operational structures.

IDaaS pricing is becoming more competitive

Downward market pressures on pricing from the newer generation of IDaaS providers is putting pressure on the pricing structures of established players such as IBM and its mainstream competitors.

Microsoft (Ovum recommendation: leader)

Figure 8: Microsoft radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

Microsoft Active Directory provides a single infrastructure for IAM

Microsoft provides pure cloud as well as a hybrid mix of cloud and on-premise IDaaS solutions that support the whole spectrum of B2E and B2B, and more recently B2C relationships. Cloud-controlled Azure Active Directory components provide portal-based access to services and applications for users and for the administration layer. On-premise bridging components are available to support directory management and directory synchronization between on-premise directories and their cloud-based equivalents. Browser and application plugins support user mobility for SSO access including the use of multi-factor and risk-based authentication.

Access management remains a key service deliverable and business protection requirement

Conditional access management is enforced using rule- and policy-based controls. These controls continue to be positioned as core business protection requirements for its clients and are key components of the Microsoft approach to IDaaS. Its facilities focus on user and device authentication, which is of particular relevance given the increasing number of mobile devices in use. This also extends to user and device compliance with usage policies, application and data sensitivity, and the associated monitoring of everyday usage patterns.

Business-focused security and user protection are core components of Microsoft's IDaaS strategy

Microsoft Azure Active Directory supports the use of risk-based, multi-factor authentication. This ties in with its support for strong access control facilities and helps deal with mobility issues and user-based controls over the devices and access channels being used. Issues such as the health and security of each device, user location when requesting access, and associated risk-based calculations (that cover issues such as the sensitivity of the data being accessed) are also being addressed. An identity and risk score is calculated for users each time an access request is made, and security alerts and reports are generated when unacceptable usage trends are identified.

Weaknesses

On-premise components appear to be the poor relation as Microsoft focuses on cloud connectivity

For on-premise identity management requirements, Microsoft offers its Identity Manager solution at no additional cost. Microsoft Identity Manager synchronizes identity between directories, databases, and applications. It provides the self-service management of passwords, user groups, and certificates; and has policy management, systems administration, and security responsibilities. However, it appears subservient to the next-generation IDaaS components.

Opportunities

IDaaS is a maturing segment of the IAM sector and Microsoft continues to build its market presence

Previous versions of Azure Active Directory focused on B2E and B2B requirements. This left a significant shortfall in the increasingly important and rapidly evolving B2C identity management space. This issue was addressed in 2015 and further developments were undertaken to deal with scalability and access control requirements for B2C coverage.

Active directory credentials can now be used to access virtual machine environments

Azure Active Directory Domain Services now supports access to virtual machines without the need to deploy domain controllers. Users that sign in to Linux and Windows virtual machine environments can use their corporate active directory credentials to provide seamless access to approved corporate assets. These approved assets are maintained using group policy controls and are based on role and departmental requirements.

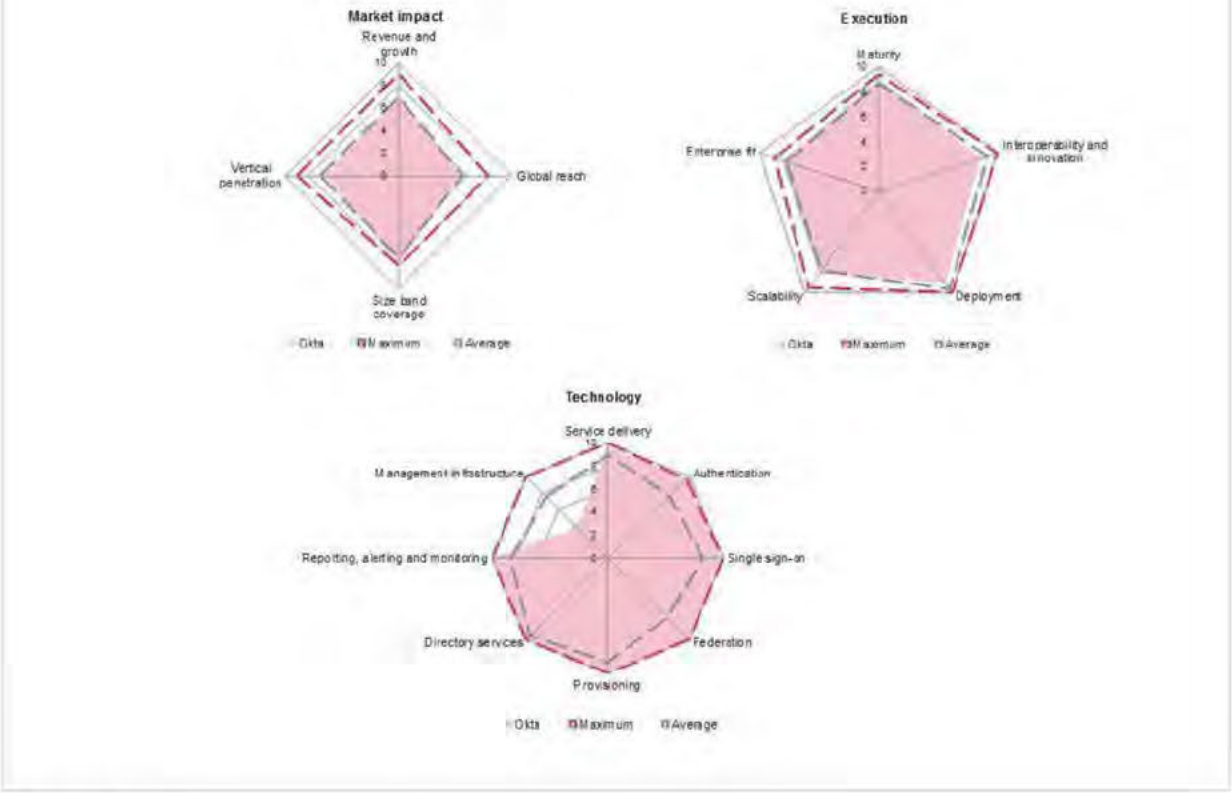
Threats

The company is still mainly perceived as a supplier of Microsoft-centric technology

Although Microsoft Azure Active Directory has been available for the last three years and its cloud directory services for at least five years, the perception remains that its identity management platforms, particularly its IDaaS services, are mainly Microsoft-centric. The company is looking to address these issues through its move to open SSO access to any cloud and its support for open protocols via its Azure Active Directory Free, Basic, and Premium editions.

Okta (Ovum recommendation: leader)

Figure 9: Okta radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

Okta covers all major IAM requirements

With provisioning, SSO, reporting, social login, identity federation, and authentication, Okta delivers all the main elements of an IAM infrastructure from the cloud. It facilitates out-of-the-box integration of its technology with cloud and on-premise apps and provides tools for third-party developers to integrate Okta into their applications.

Okta is dedicated entirely to IDaaS

Okta is not an enterprise application developer that has identity as an add-on, making it agnostic to whatever applications its customers use it to access. It architected its product from the outset for cloud delivery and so has had none of the issues of migrating an on-premise product or customer base to an "as-a-service" mode of operation. It claims the scalability to handle hundreds of millions of users.

Weaknesses

CIAM functionality should be more visible

Okta approaches CIAM by providing the foundation on which key CIAM features such as registration can be enabled through the application programming interface (API). While it produces a data stream

of identity events available for any analytics system/data warehouse, it argues that there are better tools for customer analytics than CIAM platforms because identity-related data is just one data stream of many. This is a reasonable stance, but Ovum feels it should go further to highlight its CIAM capabilities, for instance by adding registration as an out-of-the-box feature. We note that this particular capability is clearly a high priority on Okta's roadmap, and look forward to seeing it as part of the service offering in the near future.

Okta has no legacy IAM customer base

On-premise IAM heavyweights such as IBM, Oracle, and CA are moving into the IDaaS market. They have significant on-premise customer bases, which they can either migrate across wholesale over time or sell IDaaS to as an add-on capability for new greenfield projects. This option is not open to Okta, putting it at a competitive disadvantage for these accounts.

Opportunities

"Cloud-first" companies are drawn to IDaaS

Many start-ups come into existence nowadays with a "cloud-first" bias for technology acquisition. Therefore, for them, a SaaS platform for identity is clearly preferable to one that requires software to be licensed and deployed on their premises. The same goes for small greenfield projects within larger corporations, where Okta's ability to interact with on-premise corporate assets serves as a further incentive to consider its services.

The cloud is now a mainstream delivery mechanism for identity

The delivery of identity services from the cloud has become a serious alternative to on-premise IAM, particularly for start-up companies that need the benefits of identity management without the financial and operational overhead of running software in their data centers. Many large companies also approach Okta seeking the agility, scalability, and versatility offered by the cloud. Okta already has brand recognition as a leader in this space.

Threats

Okta should do more to highlight its B2C capabilities

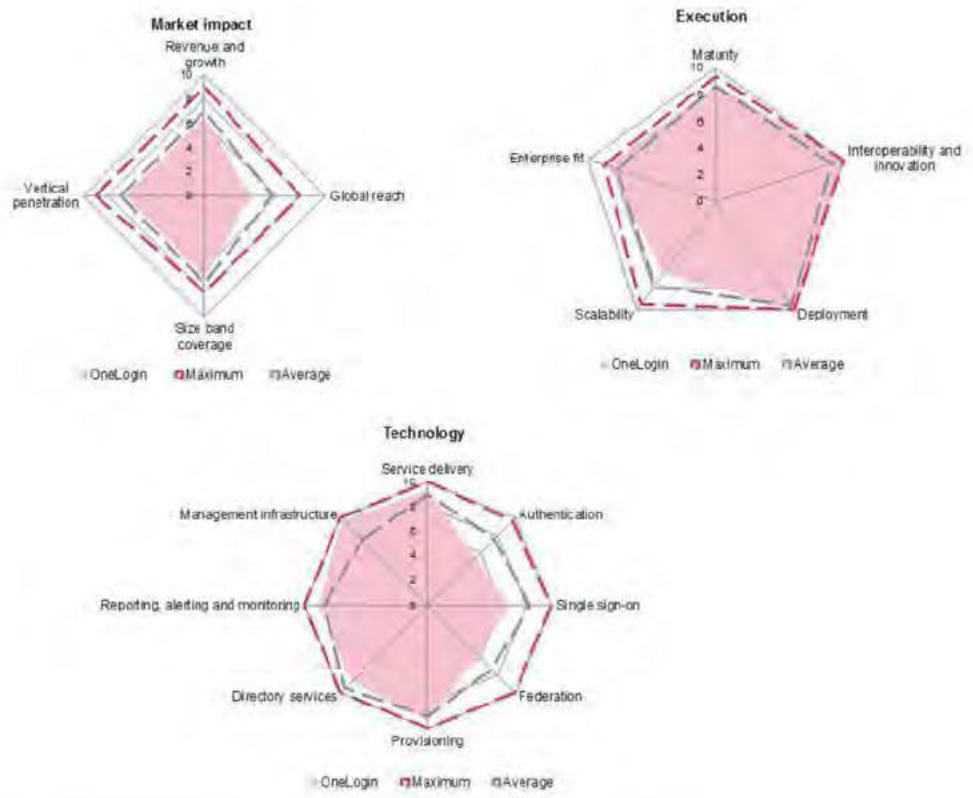
IAM started life in B2E identity services, with globalization and outsourcing taking it into the B2B sphere. The next stage is the move into B2C because customer interactions are increasingly online rather than face-to-face. Other vendors are touting their ability to address B2C requirements, and while Okta has made a good start by supporting social login, it should now productize its innate CIAM capabilities to show it is also in this market.

New IDaaS challengers come with many customers in other areas

As IDaaS becomes a serious contender for enterprise budgets against on-premise software, major players in the latter market segment are adding an IDaaS option to their technology, either by tweaking their existing platform, building an entirely new one, or buying one. Okta's ability to grow in this more competitive market may be constrained as new challengers come in with large customer bases they can leverage to expand their IDaaS business.

OneLogin (Ovum recommendation: challenger)

Figure 10: OneLogin radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

OneLogin has all the basic elements required for IDaaS

The OneLogin service is a full IDaaS offering, comprising a unified directory, identity bridging (to Active Directory, for example), user provisioning, SSO, MFA, web access management, mobile identity, device management, compliance reporting, and integration with the leading SIEMs. The company has recently moved to facilitate users' access to applications that do not support the SAML standard by acquiring password management vendor Portadi whose technology it is now adding to its platform.

OneLogin is exclusively an IDaaS vendor

OneLogin has designed and built its services for the cloud. It therefore has no legacy on-premises IAM customers and no on-premise revenues to protect. It is also solely focused on IDaaS, and so it has no other applications business, making it agnostic when it comes to connecting to enterprise applications.

Weaknesses

OneLogin lacks B2C features

OneLogin needs features for clients to manage interactions with their online customers to address the coming wave of customer IAM (CIAM), such as registration and customer behavior analytics.

Other IDaaS vendors have deeper pockets

OneLogin remains privately held and has raised a total of $42.7m. Its most recent funding round was a $25m Series C in December 2014. This compares unfavorably to the $228.5m raised to date by its largest direct competitor in IDaaS, Okta, which is currently exploring the potential for an IPO. Meanwhile, another big name in IDaaS, Ping Identity, was taken private in a $600m deal earlier this year, and it has already begun to make acquisitions. These developments make expansion for OneLogin beyond vegetative growth more challenging.

Opportunities

Cloud is the direction of travel for IAM

There is a growing requirement for identity services for employees, partners, and customers across multiple device types, and for accessing an ever-increasing number of applications. Cloud is the logical place for such functionality to reside, and the OneLogin platform is "cloud-native." There is particularly strong demand from start-ups and other small companies for IAM as a cloud service, but greenfield projects within larger enterprises may also prefer the convenience of IDaaS.

OneLogin is an established name in a growing market

The market for identity services delivered from the cloud is expanding, and OneLogin is already an established player that stands to benefit if it can keep pace with emerging new requirements and fend off competition from some of the IT heavyweights now moving into the space.

Threats

Other IDaaS platforms are adding CIAM capabilities

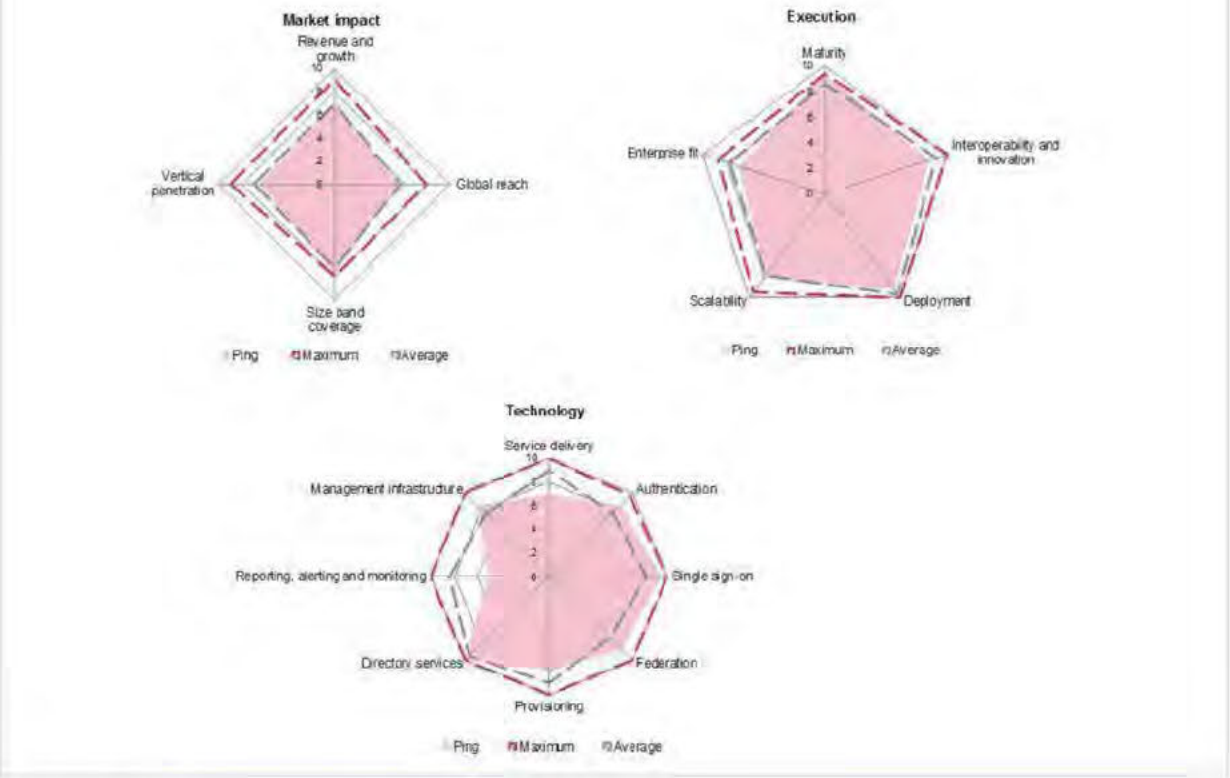
The OneLogin platform is already a broad IAM platform delivered from the cloud, as the company's 2,000 or so enterprise customers can testify. However, if it is to address the growing requirement for IAM to handle customer identities and access requirements, additional functionality will be required. One of its direct competitors, Ping, has recently acquired CIAM specialist UnboundID, and Ovum believes OneLogin needs to build or buy to keep up.

IT industry majors are moving into IDaaS

OneLogin is increasingly facing competition from larger IT industry players that are moving into the sector, such as IBM, Oracle, and CA. These companies are looking to leverage their extensive customer bases to get into IDaaS, a move that threatens to lock out OneLogin from these accounts.

Ping (Ovum recommendation: leader)

Figure 11: Ping radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

PingOne Cloud has all the elements for a fully-fledged IDaaS service

PingOne Cloud includes provisioning, SSO, MFA, directory integration, and application cataloging, making it a full IDaaS offering.

Ping is cloud-native and has just added CIAM

Ping Identity started out in 2002, enabling identity federation with its PingFederate server technology, with federation the foundation for intercompany IAM (the business-to-business or B2B side of the business). The company has since grown its platform, launching a full-blown IDaaS offering in 2012. In August this year it rounded out its CIAM capabilities with the acquisition of UnboundID.

Weaknesses

UnboundID is not yet integrated into PingOne Cloud

While Ovum applauded the acquisition of UnboundID as positioning Ping to address the expanding requirement for CIAM and to potentially span the worlds of CIAM and traditional B2E/B2B identity management with a single platform, the company now has to integrate the UnboundID technology into its own. Ping needs to carry out this process successfully and speedily for the acquisition to be a success.

Competition in IDaaS is heating up as IT majors enter the fray

The IDaaS playing field is changing. IT industry giants like IBM and Oracle are moving into the space, seeking to leverage their extensive enterprise relationships and their large customer bases in on-premise IAM. This development threatens to limit the potential for further growth for smaller vendors such as Ping, limiting their ability to penetrate enterprise accounts where there is an IAM incumbent but the customer is considering IDaaS for a new business unit, for example. Equally, companies with no legacy IAM infrastructure may be customers of the IT majors in another area of technology, representing an opportunity for them to upsell identity services.

Opportunities

PingOne Cloud benefits from a growing need for IDaaS

Ovum believes IDaaS is destined to become a major part of the IAM world, over time dwarfing on-premise software as companies move to cloud-based identity services to manage not only their employees and business partners, but increasingly also their online customers. As a full IDaaS offering, PingOne Cloud is well positioned to take advantage of this trend.

Cloud-based IAM is expanding into B2C

The cloud has become the logical place to locate identity services now that more and more enterprise applications are residing there, and access to these applications comes increasingly from outside corporate networks in the hands of remote workers, partner companies, or consumers. This trend favors providers such as Ping, and its recent acquisition of UnboundID positions the company particularly well to ride the next wave of IAM development as identity services are increasingly turned to the B2C environment.

Threats

PingOne Cloud needs to develop fast to stay ahead of the competition

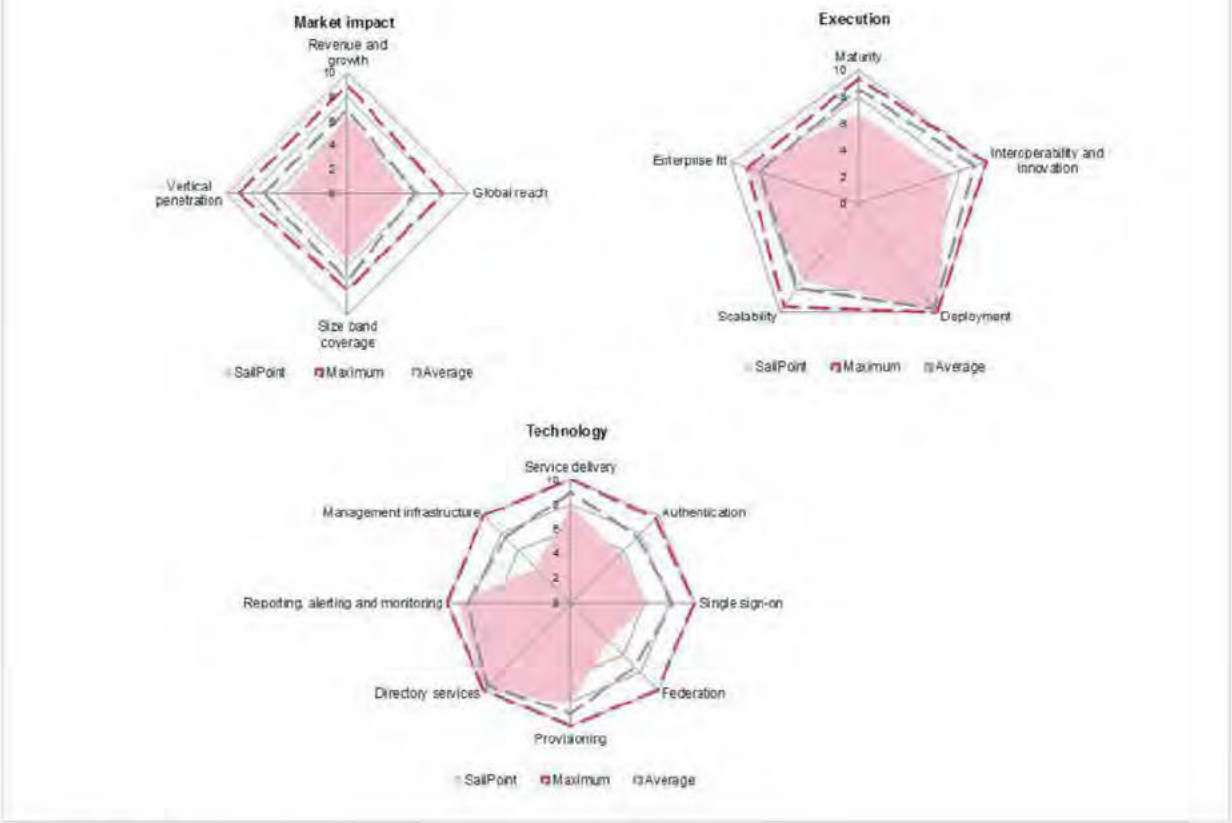
Ping Identity is a significant player in the IDaaS market, but still relatively small compared to some of the IT industry heavyweights now entering the fray. The challenge is therefore to keep PingOne Cloud up to date with the latest trends in the market, whether by internal development or by acquisition, as has just happened with the additional CIAM capabilities it got when it bought UnboundID. The company must maintain its momentum in adding new functionality to the platform lest it be overtaken by some of the larger competitors with bigger development budgets.

Competition in IDaaS is heating up as IT majors enter the fray

Ping was taken private in July this year for $600m and puts its customer base at around 1,400 enterprises. This makes it a major player at this stage in the development of the IDaaS market, but the playing field is changing. A number of IT industry giants including IBM and Oracle are moving into the space, seeking to leverage their extensive enterprise relationships and their large customer bases in on-premise IAM. This development threatens to limit the potential for further growth for the cloud-native IDaaS vendors such as Ping.

SailPoint (Ovum recommendation: challenger)

Figure 12: SailPoint radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

IdentityNow inherits SailPoint's experience with IdentityIQ

IdentityNow is a full IAM service in the cloud, with user provisioning, SSO (including support for federated SSO), password management, and access certification. With its IdentityIQ on-premise product having been in existence for the last decade, the company is transferring functionality across to its cloud platform.

SailPoint is an established IAM player

SailPoint has been in operation in the IAM market for a decade, selling to corporate entities with employee headcounts of at least 2,500. It has enterprise customers on both the on-premise and cloud sides of its business, including eight of the top 10 global banks and four of the 10 largest pharma concerns. This positions it to gauge whether existing on-premise customers want cloud-based identity services on any greenfield projects, for instance.

Weaknesses

IdentityNow is still B2E and B2B

The IdentityNow service started out with enabling companies to identify their employees and provide them with access to corporate assets (B2E). It is now also used to provide IAM services to partner

companies (B2B). However, as IAM adds functionality for online interactions with consumers (so-called CIAM), the SailPoint platform will need to add features such as registration, profile management, and customer behavior analytics.

SailPoint now needs to compete with much larger players

Since 2014, SailPoint is majority-owned by private equity firm Thoma Bravo and has been acquisitive, which suggests that its owners are prepared to spend money to support its growth and development. This will need to continue if it is to keep pace with changes in the IDaaS market, where major industry names including IBM and Oracle have entered the fray.

Opportunities

Cloud-based IAM is a growing requirement

Enterprise applications are increasingly residing in the cloud. Employees and partners access them from multiple locations and devices, most of which are not on the corporate network. The cloud is therefore the logical place from which to deliver identity services, even more so as IAM moves into the B2C world and becomes CIAM. IdentityNow can continue to ride this wave if it adds the requisite functionality.

SailPoint can grow in the IDaaS market

Demand for cloud-based identity services is growing at a healthy rate, and SailPoint is positioned to grow with it. This may require M&A activity to add functionality to keep up with the development of the market (in the CIAM space, for instance), and so far the signs are that Thoma Bravo is prepared to fund these moves.

Threats

Identity management is expanding into B2C

Although IAM started out in the B2E world, it has now expanded into B2B. With more customer interactions moving online, its next move must be into B2C, which will require new functionality to be added to platforms such as IdentityIQ and IdentityNow. Specifically, facilities such as easy self-registration, profile management, and customer behavior analytics are key features of CIAM, and SailPoint will need to address these requirements or risk staying behind market trends.

Competition is intensifying in the IDaaS market

While the IAM market is a mature and relatively stable one, the IDaaS space is rapidly becoming significantly more competitive, with heavyweights including IBM, CA, and Oracle from the on-premise world moving into cloud-based services. These are companies with marketing muscle and large existing IAM customer bases, which put pressure on smaller, more specialist firms such as SailPoint.

Appendix

Further reading

2017 Trends to Watch: Security, IT0022-000808 (October 2016)

Emerging Vendors in the IDaaS Market, IT0022-000809 (November 2016)

Author

Andrew Kellett, Principal Analyst, Infrastructure Solutions

andrew.kellett@ovum.com

Rik Turner, Senior Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo

Magic Quadrant for Identity and Access Management as a Service, Worldwide

Published: 06 June 2016 **ID:** G00279633
Analyst(s): Gregg Kreizman, Neil Wynne

Summary

Lightweight web-centric services with few identity governance and administration capabilities remain in high demand, and vendors are adding IGA features. Vendors delivering deeper functionality for IGA and legacy application support, including niche vendors, may be best for IAM leaders' needs.

Strategic Planning Assumption

By 2020, 40% of identity and access management (IAM) purchases will use the identity and access management as a service (IDaaS) delivery model — up from less than 20% in 2016.

Market Definition/Description

A vendor in the IDaaS market delivers a predominantly cloud-based service in a multitenant or dedicated and hosted delivery model. The service brokers a set of functionality across multiple IAM functions — specifically, identity and governance administration (IGA), access enforcement, and analytics functions — to target systems on customers' premises and in the cloud.

This Magic Quadrant rates vendors on their ability to be global, general-purpose IAM service providers for multiple use cases, including different types of workforce, B2C and B2B scenarios. The vendors in this Magic Quadrant must provide a baseline level of functionality in *all* of the following IAM functional areas:

IGA: At a minimum, the vendor's service is able to automate synchronization (adds, changes and deletions) of identities held by the service or obtained from customers' identity repositories to target applications and other repositories. The vendor also must provide a way for customers' administrators to manage identities directly through an IDaaS administrative interface, and allow users to reset their passwords. In addition, vendors may offer deeper functionality, such as supporting identity life cycle processes, automated provisioning of accounts among heterogeneous systems, access requests (including self-service), and governance over user access to critical systems via workflows for policy enforcement, as well as for access certification processes. Additional capabilities may include role management and access certification.

Access: Access includes user authentication, single sign-on (SSO) and authorization enforcement. At a minimum, the vendor provides authentication and SSO to target applications using web proxies and federation standards. Vendors also may offer ways to vault and replay

passwords to get to SSO when federation standards are not supported by the applications. Most vendors offer additional authentication methods — their own or through integration with third-party authentication products.

Identity log monitoring and reporting: At a minimum, the vendor logs IGA and access events, makes the log data available to customers for their own analysis, and provides customers with a reporting capability to answer the questions, "Who has been granted access to which target systems and when?" and "Who has accessed those target systems and when?"

The IDaaS market remains roughly split between two styles of offerings.

Web-centric IDaaS providers support web and mobile architected application targets in the cloud or on customers' premises. Web-centric IDaaS providers generally have strengths in multifactor authentication and SSO. Offerings tend to support the basic user administration, self-service and identity synchronization aspects of IGA, but lack legacy application connector support, and customizable multilevel approval workflow and governance features, such as access certification, role mining and role life cycle management, and segregation of duties violation detection. Web-centric IDaaS usually deploys rapidly because the services are designed to be multitenant, and customization and legacy integration requirements are not the primary design goals.

Legacy, full-featured IDaaS providers have services that were developed to support web applications on-premises and in the cloud, as well as legacy applications. More IGA connectors are available for legacy applications, and customizable approval workflows are supported. More of these vendors also provide governance features, such as access certification, role mining and role life cycle management, and detection of segregation of duties violations. Legacy-supporting implementations can be deployed rapidly, but will generally take longer and be more costly, because the more advanced IGA features they support are needed by larger organizations, often from regulated industries and with complex requirements. Also, customized IGA implementations often need implementation support from system integrators.

Over the next four years, the "fuzzy" dividing line will continue to blur as web-centric IDaaS providers deliver more IGA features that are good enough for more organizations.

Built-in or integrated enterprise mobility management (EMM) features and integration with cloud access security broker (CASB) functions are not included in this IDaaS market definition. However, Gartner notes that several vendors covered in this Magic Quadrant have integrated EMM offerings, and have either made acquisitions or have partnered for integration in the CASB market.

Magic Quadrant

Figure 1. Magic Quadrant for Identity and Access Management as a Service, Worldwide

Source: Gartner (June 2016)

Vendor Strengths and Cautions

Centrify

Centrify's Identity Service includes web-centric IDaaS, EMM and privileged access management (PAM). The IDaaS portion of the offering provides web application SSO using federation standards or password vaulting and forwarding, user provisioning, and reporting. The integrated mobility capabilities provide many of the features of stand-alone EMM vendors. Notable features include security configuration and enforcement, device X.509 credential issuance and renewal, remote device location and wiping, and application containerization. Centrify also added B2B and B2C use-case support in 2015 and 2016.

STRENGTHS

The EMM features and integration with IDaaS are the strongest among vendors in the IDaaS market that also have their own EMM capabilities.

Centrify PAM includes shared account password management and VPN-less remote session monitoring and management.

Biometric and wearable authentication options have been added, and Centrify added SSO support without requiring use of a specialized mobile SSO application.

The service and on-premises proxy component can be configured to keep some or all identity data on-premises in Active Directory and not replicate it to the cloud. Cloud identity storage is optional.

Reporting and analysis features for all events handled by the service are wide-ranging and customizable.

CAUTIONS

Centrify's B2C and B2B IDaaS offerings were new in 2015. The social identity integration provides the basics to allow a user to link and sign in with a social identity; however, social media attribute retrieval and customization of the registration and consent workflow are limited.

The vendor added single-layer, role-based approval workflow, and integrates with ServiceNow for more advanced workflows. However, as with other web-centric IDaaS providers, Centrify does not provide the governance features found in traditional on-premises IGA vendors.

Centrify has added the ability to integrate on-premises and cloud directories, such as Google's and Microsoft's; however, Centrify does not yet support customer-specific schema extensions, and its provisioning to on-premises applications is limited.

Marketing programs have been significantly bolstered in 2015 and 2016, and there has been more visibility of Centrify in the Gartner client base. However, brand awareness in IDaaS continues to lag behind primary competitors.

Centrify did well in growing its customer base, but these customers are predominantly small or midsize businesses (SMBs). Large deals, with 20,000 or more users, are rare.

Covisint

Covisint is the longest-standing IDaaS vendor in the market. Covisint's go-to-market approach is via direct sales, and also via OEM partnerships such as with Cisco, where its platform is "white-labeled" and sold under the Cisco SXP brand. Covisint got its start in the automotive industry, and provided integration broker, portal and identity services to support supply chain connectivity. Its work in the automotive industry and in supporting vehicle identities has also helped it build foundation services that can be used in other Internet of Things (IoT) applications.

STRENGTHS

Covisint Identity Manager includes user administration workflow abilities and capable administrative delegation, along with access certification features. These features were made deeper this year to support complex B2B and B2C relationships.

Covisint has shown leadership in support of IoT initiatives, particularly in the automotive industry. It continued to deepen its entity relationship management capabilities in support of IoT initiatives, specifically to support complex relationships among identities, entitlements and things.

The vendor added data centers in Germany and China to support data residency concerns in these jurisdictions, and to grow its presence in those regions.

Covisint made its service granularly accessible through microservices and APIs; it can be implemented in public or private cloud, and to support partners that white-label the offering.

Covisint can cross-sell IDaaS with its Portal, IoT and Messaging & Orchestration solutions.

CAUTIONS

Although it can support employee-to-SaaS scenarios, Covisint's focus on large customers with enterprise B2B and B2C use cases will make it a less likely choice for SMBs that are seeking workforce use-case support.

Covisint has continued to be unprofitable and has had negative net income since completely separating from Compuware in 2014, and as it had divested in nonaccretive business such as healthcare and services. Losses were less significant in 2015, and are attributed to deemphasizing participation in the healthcare space, as well as to investment in R&D to evolve its platform, and investment in sales and marketing to take to market.

Covisint seeks to sell its platform via direct sales, system integrators and OEMs. With OEMs, Covisint has white-labeled its platform as a service (PaaS), and has had early traction with Cisco and Tech Mahindra. While showing initial positive signs with some customer wins, it is too early to tell whether this strategy will succeed, and it has the potential to disintermediate Covisint from end customers.

EMC (RSA)

RSA, The Security Division of EMC, is debuting in this Magic Quadrant with its RSA Via IDaaS offering. RSA Via has coalesced from the acquisitions of Aveksa and its IGA toolset, and the acquisition of Symplified's intellectual property and some of its key staff. RSA Via Access is the service product that provides web access management (WAM) functions, and RSA Via Lifecycle and Governance is the overarching name for a set of IGA functional offerings. RSA Via's components are offered in a hybrid architecture with administrative components and multifactor authentication services mostly delivered from the cloud. The Access policy decision and enforcement points are implemented via an identity router (IDR) that can be implemented in the cloud or on-premises.

STRENGTHS

RSA has strong direct sales and reseller partnerships.

The vendor can provide SSO, multifactor authentication and full IGA functionality to support web applications, as well as provide IGA functionality for legacy applications.

RSA can take advantage of its significant SecurID customer base to cross-sell RSA Via, and the vendor has security information and event management (SIEM) and governance, risk and compliance (GRC) capabilities to cross-sell and integrate with IDaaS.

The IDR provides for encrypted passwords (for nonfederated applications) to be stored on-premises and not be held in the cloud.

CAUTIONS

The RSA Via offering has been available for one year and overall market penetration is very low.

Proven in-production references that are exercising the breadth of the RSA Via offering were not available.

The RSA Via Access and Lifecycle and Governance services, despite being marketed under one umbrella, are still technically very distinct services, with their own administration and user interfaces joined by a portal.

RSA Via can support B2C use cases, but it does not yet support OAuth and OpenID Connect (OIDC) or social identity integration, and has not yet been proven to scale to hundreds of thousands of consumers or more.

EMC is the subject of a pending acquisition by Dell. Dell has its own IAM product offerings, and RSA's sister organization, VMware, has also introduced a workforce-facing IDaaS service that includes integration of the popular AirWatch EMM toolset. It is not clear how this acquisition will alter the total portfolio of IAM offerings.

Fischer International

Fischer International, a pure-play IAM provider with a user provisioning focus, was one of the first vendors to deliver IDaaS. Fischer's capabilities are available in IDaaS, dedicated hosted, managed or on-premises software delivery models. The vendor provides functionally deep user administration and fulfillment capabilities, some governance functionality, privileged account management, and federated SSO. Its services have been particularly appealing to the higher education vertical.

STRENGTHS

Most reference customers rate the product and support highly.

Fischer's experience and native provisioning engine enable it to support granular provisioning functions for legacy on-premises applications, in addition to SaaS applications.

User administration functionality is deep, with strong connector support to a variety of directories, databases and applications, and access certification features are included. The vendor emphasizes configuration of out-of-the-box features, rather than scripting and custom development, although customers can customize the implementation. This results in rapid deployment times relative to other deep functionality vendors.

Fischer's cloud service is driven by a multitenant version of its on-premises IAM software, thus providing alternative delivery models and customer choice for the same functionality.

Fischer's scenario pricing is among the lowest, and references find that this provides solid value for the money.

CAUTIONS

Despite Fischer's long tenure in the IDaaS market, its brand recognition, market penetration and overall growth have been low compared with its competitors. Fischer's emphasis is on meeting the fundamental IAM needs of its customers, and the vendor lacks a strategy for expanding its capabilities and its presence in the global market.

Fischer has added some customers in the healthcare industry; however, the predominant focus of its marketing and sales is on the higher education vertical industry in the U.S. geographic market, and this has limited the vendor's growth in other geographies and vertical industries.

Access management is limited to SSO, without the authorization enforcement capabilities found in other IDaaS access services.

Native mobile application support is not included in the product, but is on the roadmap for 2016.

IBM

IBM's Cloud Identity Service (CIS) is provided in a multitenant model. However, components of the service can be delivered in a dedicated model. CIS is underpinned by IBM's SoftLayer infrastructure as a service (IaaS), and IBM's IAM software that delivers identity administration, approval workflow, user provisioning and access certification, along with authentication and access enforcement functionality.

STRENGTHS

IBM's functional offering is deep and aligns with the functionality provided by its software deployed on-premises.

The vendor has integrated CIS with Fiberlink's MaaS360 EMM capabilities to provide access enforcement that can use device registration and security posture to render access decisions.

IBM's breadth of resources should appeal to customers that are risk-averse and have concerns with smaller venture-funded vendors. It has geographically expanded its data center locations, and its support and professional services organizations are supporting CIS.

IBM has begun development of a variant of its offering designed for down-market customers with web-centric needs, and to support workforce-to-SaaS use cases at a more competitive price point.

CAUTIONS

Customers report that CIS can take significant effort to go live. This is partly due to the complex nature of projects that IBM takes on for larger customers.

While indicators point to the growth of IBM's offering, new clients have not yet translated into references that Gartner was able to contact.

IBM had plans to deliver its deep IGA functions (obtained as part of the CrossIdeas acquisition) as part of the CIS offering in 2015, but has continued to invest in its native IGA capabilities and has delayed a cloud-ready derivative of the CrossIdeas integration.

Despite pricing reductions in 2016, IBM's pricing for several use-case scenarios was among the highest.

Ilantus

India-based Ilantus provides IDaaS in a dedicated hosted tenant model. Ilantus began as an IAM system integrator, and has experience with traditional large-vendor IAM stacks. It offers four functional services: Xpress Access for identity administration, Xpress Governance for access governance, Xpress Sign-On for SSO and Xpress Password for password management. Xpress Access and Xpress Governance are underpinned by RSA and IBM products.

STRENGTHS

Ilantus' customer references gave the vendor high marks for implementation, support and rapid deployments again this year.

The vendor's solutions have been deployed by companies in most vertical industries, and its IGA functionality helps it support regulated industries.

Ilantus' feature set and pricing are strong for the midmarket, which is its current "sweet spot" for customer acquisition.

Xpress Sign-On for SSO provides SSO to thick-client applications, in addition to the web-architected applications that other vendors support.

CAUTIONS

The vendor has low penetration in the global IDaaS market. It has been in the U.S. market as a system integrator since 2000, but has not advanced its IDaaS offerings there or in Europe. However, it has good penetration in India, and has gained a foothold in the Middle East during the last year.

Similar to other small vendors, Ilantus lacks brand recognition and the means to increase it. It will need to step up marketing efforts and sales channel development in order to expand more rapidly internationally.

Ilantus' strategy is to focus on workforce use cases that require identity governance, provisioning and SSO to legacy targets, and to provide IDaaS at a very competitive price. The vendor will likely not be appropriate for B2C use cases in the short term.

The vendor's roadmap plans are incremental and mostly designed to keep service on par with current competitors' capabilities.

iWelcome

Netherlands-based iWelcome provides its IDaaS in a dedicated single-tenant delivery model to allow for customization and customer branding. Its offering includes authentication, SSO, federation, self-service registration and user provisioning support for on-premises and SaaS applications.

STRENGTHS

iWelcome is the only established IDaaS vendor rated in this Magic Quadrant with headquarters located in continental Europe. The vendor has data center presence in nine European countries, and continues to expand European data center coverage for resiliency and to meet stringent European data residency requirements.

The vendor has strong capabilities in access management — particularly in authentication, federation protocol and identity repository support.

iWelcome has grown a significant portion of its business by supporting B2C use cases, and owes this success to consumer-oriented features such as social registration and login, consent management, service desk automation, configurability of the user experience, and event and data reporting.

It has been rearchitecting its platform for microservices to support improved deployment and release automation, as well as the demands for customization and configuration per customer.

CAUTIONS

iWelcome lacks core identity governance features (such as access certification and recertification), and its provisioning approval workflow capabilities are minimal. The vendor relies on integration with customers' established IGA toolsets.

Its overall customer base is small, compared with most competitors, although it grew the business proportionately well for its size during 2015.

In 2015, iWelcome refocused its sales and marketing strategies to be more direct, and they are augmented by a few strategic partnerships. These efforts will need to expand rapidly in order to compete effectively.

The vendor began providing solution architect and dedicated customer success staff for each engagement — an improvement over last year. Existing customers report that the platform is reliable and performs well, but that technical support could be more responsive.

iWelcome has extended its business-to-employee (B2E) proposition to become a consumer IAM provider that delivers functionality based on microservices and tailored to each customer. This provides flexibility for distinct customer needs, but will make it difficult to compete against vendors that have been able to deliver repeatable, general-purpose in-demand functionality.

Microsoft

Microsoft's Azure Active Directory Premium offering provides features that are in line with other web-centric IDaaS providers, and includes licenses for Azure Multi-Factor Authentication (MFA). It also includes licenses for Microsoft Identity Manager (MIM) that are to be used with customers' on-premises systems. Microsoft also offers Azure Active Directory Premium as part of its Enterprise Mobility Suite (EMS), along with Microsoft Intune EMM and Azure Rights Management, and the on-premises-based Advanced Threat Analytics tool.

STRENGTHS

Microsoft continues to leverage its current and substantial customer base for Office 365 and other products to add Azure Active Directory and EMS to contracts. The vendor has broad and deep marketing, sales and support capabilities, and it has been pricing EMS low, which has put significant pressure on other IDaaS players.

The vendor has already demonstrated high scalability with Azure Active Directory. The service underpins other Microsoft Azure services.

Microsoft has a strong international presence for its service offerings, and continues to expand its IaaS presence worldwide.

Through acquisition and development, the vendor has demonstrated advancement of its strategy to secure identities, data and devices.

Microsoft's strategy demonstrates a strong understanding of the technology, socioeconomic, security and jurisdictional trends that will shape its offerings going forward.

CAUTIONS

The Azure Active Directory B2C and B2B Collaboration subservices were in public preview (beta) at the time our analysis was performed. These offerings will likely need time to mature relative to competition with established B2C and B2B use-case support.

Microsoft's on-premises "bridge" components for synchronization and federated SSO are now managed under one umbrella component, Azure Active Directory Connect. However, based on Gartner client interactions, these components generally need more infrastructure and more effort to manage than competitors' bridge technology.

Microsoft can manage the transition of organizations with multiple Active Directory forests to one tenant of Office 365; however, Gartner client feedback is that this transition is easier with competitors' IDaaS offerings.

Microsoft lags behind competitors in the number of apps it can provision to, as well as the depth of SaaS account fulfillment that supports the provisioning of roles, groups and other attributes.

Okta

Okta's IDaaS offering is delivered multitenant, with lightweight on-premises components for repository and target system connectors. IDaaS is Okta's core business. The vendor delivers basic identity administration and provisioning capabilities, access management for web-architected applications using federation or password vaulting and forwarding, and reporting. Okta also provides adaptive multifactor authentication capabilities, including its own phone-as-a-token solution. The vendor added an integrated mobility management product in 2014.

STRENGTHS

Okta's marketing and sales strategies have been effective, as demonstrated by brand recognition and an increased volume of customers. Its customer base continued to grow significantly in 2015 and early 2016.

The vendor's continued investment in its platform for developers has paid off, and now a significant portion of its business supports integrations with customers' applications and workflows.

References and Gartner clients have continued to report predominantly positive experiences with rapid implementation, reliability and support.

Okta's addition of European data centers, its ISO 27001 certification and its adherence to EU model law should assuage some concerns about data protection.

CAUTIONS

Okta began to enhance its user provisioning functionality to add multilevel approval workflow, but will need to continue to add features found in traditional IGA tools to gain replacement business from customers with traditional IGA tools on-premises.

Okta's reporting capabilities are limited relative to competitors.

The vendor slightly increased the portion of its business that comes from Europe and the Asia/Pacific region; however, Okta's current customer base is predominantly located in the U.S.

While Okta's market penetration and proven implementations have greatly outpaced most competitors, the vendor is venture-funded and details of its profitability are not yet public. This is likely to be a watershed year for Okta, as it continues to face intensified competition from Microsoft and other vendors.

OneLogin

OneLogin's service architecture is multitenant, and lightweight integration components are used for on-premises connections. IDaaS is OneLogin's core business. The vendor delivers basic identity administration and provisioning capabilities, access management for web-architected applications using federation or password vaulting and forwarding, and reporting.

STRENGTHS

OneLogin significantly expanded its customer base in 2015 and early 2016, and has some large customers, although the majority of its clients are SMBs.

OneLogin delivers a virtual LDAP services that enables application servers, VPN and Wi-Fi networking components that need LDAP authentication and attribute retrieval to use OneLogin as an LDAP server.

OneLogin purchased Cafesoft in late 2015 and now delivers a full-featured on-premises WAM tool to support proxy- and agent-based access to customers' on-premises web apps.

The vendor has leveraged its venture funding to expand sales, marketing and support to non-U.S. geographies, and has expanded its use of partner channels to enable sales.

References were solid, and appreciated the support and service reliability they received from OneLogin.

CAUTIONS

OneLogin continues to face increased competition from larger competitors. The vendor is venture-funded and details of its profitability are not yet public. Pricing pressure from other vendors in the market is likely to increase time to profitability.

OneLogin maintains a singular focus on IDaaS. The vendor provides the rudiments of mobile device management (MDM), such as device registration, certificate management and certificate-based SSO for Macintosh and Windows clients, and mobile endpoints are on the roadmap. However, the service lacks broader device management capabilities. This could make it difficult to compete against vendors with broader offerings.

Canned and customized reporting capabilities are basic relative to most other vendors in the market.

OneLogin lacks its own deep user administration and provisioning and identity governance functionalities.

Ping Identity

The PingOne Cloud service is a multitenant web-centric IDaaS offering that Ping Identity targets toward large enterprises. Ping Identity provides a lightweight self-service bridge component to integrate a customer's Active Directory to the service, and also uses the well-established PingFederate product as the on-premises bridge component for customers when broad protocol and directory support are needed. In addition, PingAccess can be deployed to support proxy access to internal web applications and APIs. PingOne Cloud includes PingID, a multifactor authentication service that can utilize contextual data for authentication, such as location, network, biometric and device data. On 1 June 2016, Ping Identity announced that it was acquired by Vista Equity Partners. The transaction is expected to close in the third quarter of 2016.

STRENGTHS

By leveraging the PingFederate technology for the bridge component, Ping Identity can provide SSO by integrating with a variety of identity repositories, existing customer access management systems and target application systems.

Ping Identity has demonstrated support for multiple workforce and external identity use cases.

The vendor has shown strong leadership in identity standards development, as well as openness in working with customers and competitors to evolve those standards.

Ping Identity has broad vertical and geographic market penetration through its value-added reseller (VAR) and system integrator partner networks; also, it has made inroads with managed service providers that can offer PingOne Cloud functionality.

CAUTIONS

PingOne Cloud is one of the services with strong access features, but lightweight IGA capabilities. User self-service access request, provisioning workflow and most identity governance features are missing.

Ping Identity's strategy of continued R&D focus on access management, authentication, federation and standards is laudable; however, the vendor has decided to pursue a strategy of partnerships and integrations in the areas of IGA and MDM, which may meet the needs of some global enterprises, but leaves Ping Identity vulnerable to competitors.

The vendor's reporting capabilities are weak compared with most competitors.

SailPoint

SailPoint IdentityNow features access request and provisioning, access certification, password management, authentication, and SSO service elements. The architecture is multitenant and can deliver services completely in the cloud, and it can be bridged to enterprise environments to support on-premises applications.

STRENGTHS

SailPoint's legacy of providing strong on-premises IGA has helped it deliver a subset of the functionality from the IdentityIQ product in IdentityNow. Responsive user interfaces have been added to help IdentityNow capabilities to be managed and used easily across traditional and mobile endpoint devices. Solid and flexible access certification features were added this year.

SailPoint's full complement of provisioning connectors provides fulfillment capabilities to a wide variety of identity repositories and target systems, and significant product updates have been made to the password management functionality.

SailPoint has a broad geographic presence for sales and support as a foundation for selling its IDaaS, and it has added data centers in Europe and Sydney. Its administration and user interface internationalization has progressed commensurately with sales.

The vendor is profitable, and Thoma Bravo became a majority owner in SailPoint in 2015, thereby bringing additional resources to it.

CAUTIONS

SailPoint's IDaaS market share is growing, and it picked up some large customers; however, overall market penetration is still low relative to IDaaS competitors.

IdentityNow does not support social identity use cases, and is not a strategic fit for organizations seeking consumer-facing IAM solutions.

Despite its strength in IGA and the addition of significant access certification functionality, approval workflow is still missing from IdentityNow. This feature set continues to be on the roadmap.

IdentityNow is limited in its ability to support delegated administration for B2B use cases.

Salesforce

Salesforce provides Salesforce Identity as part of its Salesforce PaaS. It sells Salesforce Identity as an independent service offering, but also includes it for established Salesforce customers. Identity Connect is Salesforce's on-premises bridge component that is sold separately. The service includes the baseline functionality required for inclusion, as well as social registration and login, federation gateway functionality, and deep access request and user provisioning workflow functionality.

STRENGTHS

Salesforce is able to place some commoditization pressure on the market by including IDaaS functionality in its core offering, thereby providing incentives to keep its customer base from being drawn to alternatives — at least for consumer-facing use cases.

Salesforce Identity takes advantage of customization capabilities inherent in the platform including the deep access request and approval workflow functionality

Salesforce Identity includes contextual multifactor out-of-band authentication service as a result of its acquisition of Toopher in 2015.

Salesforce Identity has strong social media and identity standards support, including SAML, OAuth2, OIDC and SCIM, and the vendor actively participates in standards bodies, including IETF and the OpenID Foundation.

CAUTIONS

The vendor does have some "identity only" customers, but the majority of users are established Salesforce platform customers.

While Salesforce Identity can support provisioning and SSO to on-premises applications and SaaS apps, it lacks a password vault and the service has fewer provisioning connectors than leading vendors, making the breadth of application support limited relative to competitors.

Market penetration for Salesforce Identity is predominantly for B2C and B2B use cases, and workforce use-case implementations are rare.

Salesforce Identity does not provide proxy-based access to on-premises web applications, nor does the bridge component of Salesforce Identity provide the ability to synchronize cloud directory changes from its cloud directory back to enterprise directories. Professional services are needed to deliver this functionality.

Simeio Solutions

Simeio Solutions provides a mixture of dedicated hosted and on-premises managed service offerings. Its services are underpinned by products from other well-established IAM software vendors, which allows the vendor to provide WAM; identity administration; access request; role and compliance; privileged account management; risk intelligence; IT governance, risk and compliance services; and directory services. The vendor provides its own overarching administration components and identity bridge that integrate with underlying products from other vendors.

STRENGTHS

Simeio's use of major IAM stack vendors' technologies provides it with an arsenal of products that delivers deep functional support for web and legacy applications. The same vendor partnerships provide referrals to Simeio for customer acquisitions.

The vendor operates Identity Intelligence Center, an operations center overlay that provides actionable insight into patterns of usage among users that may exist across multiple vendor identity sources and other security systems.

Simeio's history as an integrator has given it the experience to help customers plan, design and integrate their IDaaS offerings. The vendor continues to enhance its administration and user interfaces as abstraction layers among the multiple underpinning vendors' technologies to help with consistency and time to value with implementations.

The vendor's service-based roots have enabled it to have a positive cash flow since its inception. A cash infusion last year has helped Simeio to fund marketing, sales and R&D efforts.

Simeio has a good spread in its vertical industry and geographic representation.

CAUTIONS

Simeio's organization and its overall customer base grew in 2015 and early 2016, but not as rapidly as those of vendors selling web-centric solutions.

The vendor's use of OEM software requires the incorporation of those third-party vendors' software licensing costs in its offerings. This tends to make Simeio's pricing high for pure web application use cases.

Simeio is still relatively unknown in the IDaaS marketplace, but is slowly building its customer base and brand awareness, thanks to vendor partners — some of which are also competitors.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

EMC (RSA)

Dropped

CA Technologies — CA delivers IAM capabilities on-premises and as a hosted service through its partners. Its new IDaaS offering is currently in controlled release and planned for launch later this calendar year.

Exostar — Exostar's almost exclusive focus on supporting B2B use cases excluded it from this Magic Quadrant, which evaluates vendors that are delivering IAM functionality to support multiple use cases.

Inclusion and Exclusion Criteria

The vendor must provide a minimum level of functionality in all the IAM functional areas outlined in the Market Definition/Description section.

Vendors that deliver only one or two of these core IAM functions as a service, such as authentication only, were not covered as part of this research. The following additional inclusion criteria were used:

Longevity of offering: Each IDaaS offering has been generally available since at least 31 December 2015 and is in use in multiple customer production environments.

Origination of offering: The offering is manufactured and operated by the vendor, or is a significantly modified version obtained through an OEM relationship. (We discount any service offering that has merely been obtained without significant functional modification through a licensing agreement from another vendor — for example, as part of a reseller/partner or service-provider agreement.)

Number of customers and end users (including customers of third-party service providers and their end users): As of 31 December 2015, the vendor had:

More than 20 different active customer organizations using its IDaaS offerings in a production environment

Revenue attributed to fees for IDaaS service usage that was greater than $4 million for the year ending 31 December 2015

Verifiability: Customer references must be available.

This Magic Quadrant does not cover the following types of offerings:

Remote or on-premises "managed" IAM — services designed to manage customers' owned or hosted IAM infrastructure.

IAM functions provided only as part of a broader infrastructure or business process outsourcing agreement. IDaaS must be provided as an independently available and priced service offering.

Vendors that provide predominantly B2B services and, therefore, do not have significant presence in the market that provide general-purpose IAM services that support workforce or B2C use cases as well.

Other Vendors of Note

There are some vendors that did not completely meet the inclusion criteria for this Magic Quadrant or were vendors that had little or no Gartner client interest. However, these vendors may support one or more use cases very well. Bitium, Gigya, Intermedia and Janrain will be covered in companion Critical Capabilities research to be published shortly after this Magic Quadrant.

Bitium and Intermedia offer a web-centric IDaaS, but only support the workforce-to-web-application use case.

There has been some Gartner client interest in two vendors, Gigya and Janrain, that specialize in consumer-facing IAM, and particularly social identity integration.

Optimal IdM is somewhat more well-known for its on-premises virtual directory and federation solutions. It has moved its solution to an IDaaS model. Optimal IdM's IDaaS offering is relatively unknown in the Gartner client base; however, it is delivered in a private cloud that can be customized to meet customers' needs.

Evaluation Criteria

Ability to Execute

Product or Service:

The service's overall architecture, with emphasis on the service's global availability and resiliency features, and its flexibility to support on-premises identity repositories and cloud-only implementations. The level of support and expertise required by customers to help maintain the components. The extent to which a service's functions are exposed via APIs for customers' system integration.

Security and privacy: The physical and logical controls implemented by the vendor and any underpinning IaaS provider; security for on-premises bridge components and connections between the bridge and the IDaaS; controls for data security, particularly regarding personal information; and vendors' third-party certifications received for the services.

The variety of on-premises and cloud identity repositories that can be supported, and the quality of integration with same. The ability of vendors' cloud directory schemas to be extended by customers to support customers' needs.

The depth and breadth of IGA functionality:

Access request

Access approval workflow depth and functionality

Access certification

Attribute discovery and administration

Administrative access enforcement — for example, to identify, alert and prevent inappropriate access

Provisioning create, read, update, delete (CRUD) user identities and entitlements to target systems

Configuring target system connectors

The depth and breadth of access functionality:

User authentication methods supported

Breadth of SSO support for target systems

Federation standards

Support for mobile endpoints and native mobile application integration

Authorization enforcement

The depth and breadth of identity monitoring and reporting:

- Canned reporting
- Customized reporting
- Data export to on-premises systems
- Analytics

Integration with Microsoft Office 365, Microsoft SharePoint, customers' on-premises VPNs and WAM systems

Deployment requirements, such as speed of proof of concept and deployment, customer staffing requirements, and factors that add complexity and may affect speed to deployment and staffing.

Overall Viability:

Overall financial health

Success in the IDaaS market in terms of the number and size of customer implementations; this aspect is heavily weighted

The vendor's likely continued presence in the IDaaS market

Sales Execution/Pricing:

The vendor's capabilities in areas such as deal management and presales support, and the overall effectiveness of the sales channel, including VARs and integrators

The vendor's track record in competitive wins and business retention

Pricing over a number of different scenarios; this aspect is heavily weighted.

Market Responsiveness/Record:

The vendor's demonstrated ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act and market dynamics change.

How the vendor can meet customers' evolving IDaaS needs over a variety of use cases

How the vendor has embraced standards initiatives in the IDaaS and adjacent market segments, and responded to relevant regulation and legislation

Marketing Execution:

The clarity, quality, creativity and efficacy of programs designed to deliver the vendor's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This mind share can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities. For example:

- Marketing activities and messaging
- Visibility in the press, social media and other outlets
- Vendor's appearance in vendor selection exercises, based on Gartner client interactions

Customer Experience:

Customer relationship and services

Customer satisfaction program

Customer references; this evaluation subcriterion was weighted heavily and included input from vendor-supplied references, as well as unsolicited feedback from Gartner client interactions

Operations

People — that is, the size of the organization and the track record of key staff members

Quality and security processes

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	Low

Source: Gartner (June 2016)

Completeness of Vision

Market Understanding:

Understanding customer needs: Methods, the effects of the Nexus of Forces (cloud, mobile, social and information), and the IoT

The future of IDaaS and the vendor's place in the market, as well as the vendor's views on top technological, nontechnological and regulatory changes in the market

Marketing Strategy:

Communication and brand awareness: The clarity, differentiation and performance management of the vendor's marketing messages and campaigns

The appropriateness of the vendor's use of events, social media, other online media and traditional media as part of its marketing efforts

Sales Strategy:

The vendor's strategy for selling its IDaaS offerings that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates, which extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy:

The vendor's approach to developing and delivering its IDaaS offerings, which meet customers' and prospects' needs with respect to their key selection criteria, and the needs created by cloud computing, mobile computing, social media, digital business and other market dynamics. Also, the vendor's ability to exploit the Nexus of Forces to improve its IDaaS products and services.

The strength of the vendor's roadmap, and how the vendor will increase the competitive differentiation of its IDaaS and ancillary services.

Business Model:

The soundness and logic of the vendor's underlying business proposition:

The vendor's views of key strengths and weaknesses relative to competitors

Recent company milestones

Path chosen for future growth and profitability

Vertical/Industry Strategy:

Customer breadth and penetration into various industries and sizes of customer organizations:

Views of industry trends and special needs

Strategy for expanding IDaaS adoption in different industries

Innovation:

Foundational technological and nontechnological innovations

Recent and planned innovations

Organizational culture and how it affects innovation

Geographic Strategy:

Global geographic reach of customer base and trends

Strategy for expanded geographic customer acquisition

Global nature of technical support and professional services, and language internationalization for administrative and user interfaces

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Medium
Marketing Strategy	Medium

Evaluation Criteria	Weighting
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Low

Source: Gartner (June 2016)

Quadrant Descriptions

Leaders

Leaders in the IDaaS market generally have made strong customer gains. They provide feature sets that are appropriate for current customer use-case needs. Leaders also show evidence of strong vision and execution for anticipated requirements related to technology, methodology or means of delivery. Leaders typically demonstrate solid customer satisfaction with overall IDaaS capabilities and/or related service and support.

Challengers

Challengers also show strong execution, and have significant sales and brand presence. However, they have not shown the Completeness of Vision for IDaaS that Leaders have. Rather, their vision and execution for technology, methodology and/or means of delivery tend to be more focused on or restricted to specific functions, platforms, geographies or services. Challengers' clients are relatively satisfied, but ask for additional functionality, more timely support and higher service levels than are currently delivered. There are no Challengers in this Magic Quadrant.

Visionaries

Vendors in the Visionaries quadrant provide products that meet many IDaaS client requirements, but they may not have the market penetration to execute as Leaders do. Visionaries are noted for their innovative approach to IDaaS technology, methodology and/or means of delivery. They may see IDaaS as a key part of a much broader service portfolio. They often may have unique features, and may be focused on a specific industry or specific set of use cases. In addition, they have a strong vision for the future of the market and their place in it.

Niche Players

Niche Players provide IDaaS technology that is a good match for specific use cases. They may focus on specific industries or have a geographically limited footprint, but they can actually outperform many competitors. Vendors in this quadrant often have relatively fewer customers than competitors, but they may have large customers as well as a strong IDaaS feature set.

Pricing might be considered too high for the value provided by some niche vendors. Inclusion in this quadrant, however, does not reflect negatively on the vendor's value in the more narrowly focused service spectrum. Niche solutions can be very effective in their areas of focus.

Context

Vendors evaluated in this Magic Quadrant come from distinctly different backgrounds. Their pedigrees vary greatly, as do their abilities to provide IAM functional depth and support for different use cases. Their aspirations for servicing customers by geography, industry and customer-size segmentation also vary.

Clients are strongly cautioned not to use vendors' positions in the Magic Quadrant graphic (see Figure 1) as the sole source for determining a shortlist of vendors. Vendors were evaluated with regard to their ability to provide a general set of IAM functionalities across multiple use cases, and in multiple geographies and industries, and to do so by providing solid value for money as perceived by their customers. All vendors covered in this Magic Quadrant have succeeded in providing customers with services that meet their needs. However, client requirements — particularly those for IAM functional depth, speed to implementation, geographic coverage and price — are most likely to strongly affect their choices for a shortlist:

1. Clients focused on web-architected application targets and employee-to-SaaS use-case application needs should strongly consider Centrify, Microsoft, Okta, OneLogin and Ping Identity. Currently, however, these vendors have limited IGA abilities. They tend to lack multilevel provisioning approval workflows, as well as identity governance features such as access certification, segregation of duties violation detection, or role engineering and certification. These vendors' provisioning connectors for legacy application targets are also lacking.
2. Clients focused on consumer-facing IAM use cases should strongly consider Covisint, IBM, iWelcome Okta, OneLogin and Salesforce.
3. Clients that need more functional depth in IGA and legacy on-premises application targets should strongly consider EMC (RSA), Fischer International, IBM, Ilantus, Simeio Solutions and SailPoint. More of these vendors also provide dedicated hosted instances of their offerings as options.

Clients generally should expect more complex, time-consuming and costly implementations when they have requirements for IGA functional depth, and when they have legacy (non-web-architected) on-premises application targets. These requirements generally indicate a stronger need for IAM process and data modeling and target system integration functions, such as connector development and configuration.

System integrators have been needed when clients implemented traditional IAM software suites with these types of requirements. Several of the vendors listed above in No. 3 come from system integration backgrounds. IDaaS customers should expect best practices and operational excellence from them due to their familiarity with the software components that underlie the solutions. There should be some deployment and integration efficiency gains relative to do-it-yourself approaches.

However, customers should not expect to easily "forklift" an existing, complex IAM implementation with multiple IGA workflows and many legacy system connectors to the cloud without significant integration work and quality assurance testing. Dedicated per-client IAM infrastructure also drives up the cost of the offering relative to multitenant offerings. The cost of underlying IAM third-party software licenses also may drive up the overall costs of the implementation.

Security

Gartner clients rightly express concerns with regard to identity data security and protection of enterprise users' passwords when IDaaS is being considered. The following are generally true for IDaaS security practices, with some exceptions:

Some user identity data will be held in the cloud. Most commonly, this data includes first and last names and email addresses. Some vendors, such as Centrify and Ping Identity, require no user attributes to be held in the cloud, with the assumption that all data needed for provisioning users to SaaS application targets is held in the on-premises directory and can be accessed by the vendors' bridge components. Centrify offers on-premises-only or hybrid cloud implementation, and the hybrid implementation requires some identity data to reside in the cloud. Ping Identity's solution works similarly. Generally, as the number of attributes needed to provision users' accounts grows, that data must at least pass through vendors' IDaaS services in order to be provisioned to SaaS targets. A cloud-only implementation of IDaaS must hold all these attributes.

Data is encrypted in transit over networks. However, one exception is that passwords are sent in the clear during transmittal to target systems when federation is not supported, and Secure Sockets Layer (SSL) or Transport Layer Security (TLS) are not used between the browser and target system. This is essentially the same as when a user's browser interacts directly with an application without IDaaS controlling the access. Also, SSL usually is used for SaaS sign-on flows, whether an IDaaS is brokering the access or not.

Identity data in the vendor's cloud is encrypted at rest. Vendors have different strategies for managing encryption keys. Most vendors generate different encryption key pairs for each customer's instance of the service, and there is variance in how those keys are managed. Technically, the keys may be under the customer's strict control, or the vendors' operations staff may control the keys. In the latter case, the vendors claim that their personnel will have other controls in place to ensure that there is no inappropriate use of the keys.

On-premises bridge components will use SSL/TLS to communicate with the service, and many of the vendors will require no inbound firewall port to be opened to support this. Communications are initiated outbound from the bridge.

With few exceptions, providers use IaaS providers, rather than their own operations centers, to host their offerings. All vendors maintain some type of third-party security certification, as do the IaaS providers that host the IDaaS. SOC 2 is common. ISO/IEC 27001 is becoming more common.

No security is perfect. Ultimately, prospective customers must decide whether vendors' stated control sets are sufficient for their needs. IDaaS vendors give significant attention to ensure the security of their platforms. Based on the number of enterprise security breaches that have been

made public, and the lack of any such breaches for IDaaS providers, Gartner believes that IDaaS vendors are more likely to provide better security for IAM services than their customers could provide for themselves (see "Predicts 2016: Cloud Computing to Drive Digital Business").

Availability

The use of IDaaS may introduce a single point of failure. IDaaS vendors generally have taken care to architect their services with network and system redundancy features, and to host their services on an IaaS that has been provisioned with sufficient redundancy to guarantee adherence to IDaaS vendors' service-level agreements. Also, IDaaS vendors have generally architected their on-premises bridge components to be implemented redundantly, if customers choose to do so.

Nevertheless, a major system failure with IDaaS has the potential to temporarily leave customers without access to the applications that IDaaS serves. Organizations face similar risks when they manage their own IAM services, and when components such as federation servers fail. Overall adherence to service levels improved during 2015 and into 2016, with references reporting solid availability across the board.

Clients that choose to accept the risks of using IDaaS should have an emergency business continuity process in place that includes these steps:

- Bring up any available in-house federation technology and federate to key target systems, if possible.
- If federation services are not available, then temporarily turn off federation at target systems and fall back to password-based authentication.
- Issue temporary passwords for all target application accounts that can support password-based authentication.
- Fall back to manual user provisioning processes.

Data Residency

Most of the vendors covered in this research are U.S.-based. Gartner clients from other countries may have concerns about employees', business partners' and customers' personal data that could be held in the cloud. Despite the use of local or regional data centers to host services and data, international clients still may be concerned about the U.S. government's ability to get access to the data. This is currently a risk that clients must evaluate, and then determine whether it is acceptable. All vendors are aware of the European action around Safe Harbor and the impending Privacy Shield directive, For clients that intend to use IDaaS, but have concerns about U.S. providers, we recommend that European IDaaS or managed service providers be used. There are also early examples of U.S. IDaaS vendors' offerings being separately white-labeled and managed by European providers. Alternatively, we recommend that clients require U.S. vendors to sign the EU's model contracts on privacy, and require your ownership of encryption keys. If possible, evaluate the controls associated with the development and operations staff, and their access to the keys.

Pricing

Gartner asked vendors to provide "street" price quotes for several use-case and volume usage scenarios. Vendors were cautioned against providing list prices. However, some vendors chose to respond with list prices. Vendors were asked to provide all costs, including startup costs, over a three-year subscription period. Three of the most commonly required scenarios are included below, with a range of costs and averages. Gartner clients should use the figures below for budgeting purposes. However, we recommend that clients treat the pricing below as budgetary, and should expect to pay significantly less (on average) than these figures would indicate, due to the inflated prices that some vendors chose to deliver for our surveys. Gartner's observations of the price quotes submitted by our clients have corroborated this finding.

Scenarios No. 1 and No. 2: 1,000-Employee and 10,000-Employee Workforces, Web-Architected Applications

Number of users: 1,000 in the workforce ("any" staff) who use the service several times daily.

Endpoints: Company-owned PCs; approximately 60% Windows Active Directory and 10% Mac OS X, 30% mix of Apple and Android tablets and smartphones.

User location: Could be anywhere — a mix of on-premises corporate LAN and external use cases.

All identities and attribute data are held in Active Directory.

Support to: Five externally hosted (SaaS) applications and five internal web application targets.

Allow the company's administrator to directly manage users' identities, and provision these to Active Directory. Subsequently and automatically provision accounts to the five SaaS applications, with the assumption that there is an available provisioning API for all five, and that the vendor already has created provisioning connectors for three of the five applications. Two of the applications need connectors created for the customer.

User self-service application access request, administrator approval, subsequent provisioning as described above, and user self-service password reset.

User authentication to the service and SSO to all target applications, three using SAML federation and two using password vaulting and forwarding; support for identity-provider-initiated federated SSO to your service, based on an Active Directory authentication; and service-provider-initiated redirect authentication for an externally located user who connects to SaaS first, and to support authentication against your service and corporate Active Directory.

Reporting for all administrative and access events.

We requested pricing for two variants. Scenario No. 1 included support of the above requirements for 1,000 internal users. Scenario No. 2 included support of the above requirements for 10,000 users, with the added requirement that 5,000 of those users be provided with SMS or voice-based OTP authentication. The results:

The average three-year cost of the 1,000-user scenario was $196,045.

The average three-year cost of the 10,000-user scenario was $677,920.

In both scenarios, vendors that had significant gaps in the required functionality were removed from the average calculation, as were the high pricing and low pricing that were significantly out of line with the other vendors' pricing.

Scenario No. 3: 1,000,000-User, Consumer-Facing

Gartner client interest in support for B2C use cases increased this year, and we altered the scenario pricing evaluation to focus on a representative scenario:

1,000,000 consumer users.

Usage: once monthly on average by each user.

Endpoints: any endpoint with web browser from any location.

Authentication and SSO are provided to three internal on-premises web applications, and two SaaS applications. Social identities can be registered, linked to established identities and used for subsequent authentications.

Identity data is held in the IDaaS vendor's cloud directory or on the customer's premises.

Self-service user administration and password reset are provided.

Automated user provisioning to any approved application is provided, with the assumption that all targets have a provisioning API available.

Reporting is provided for all administration and access events.

The average three-year cost of this scenario was $807,674.

In all cases, clients are strongly encouraged to understand their own total costs of ownership for managing the same IAM functions in-house, so that these costs can be compared with IDaaS pricing. Gartner also collected pricing data for other scenarios, including those requiring more in-depth IGA functionality and legacy on-premises application support. Pricing was highly variable for these implementations. Clients interested in these scenarios should contact Gartner for more information.

Trends

Here, we discuss the key trends that are shaping the IDaaS market, and how the market will evolve.

Web-Centric IDaaS Leads the Market in Terms of Customer Acquisition

Web-centric IDaaS vendors continue to make solid gains in the market. Gartner estimates that 90% to 95% of client interactions on the topic of IDaaS indicate a need for web-centric solutions to support B2E SaaS target system integration and consumer-facing and consumer use cases. Ten percent of interactions indicate a need for more full-featured B2E IDaaS with legacy on-premises application support and IGA needs.

As web-centric vendors have moved upmarket, they find that larger organizations tend to have existing IAM software solutions in place and the staff to manage those solutions. These prospects, which may wish to extend their current implementations with IDaaS, or which are hoping to replace their on-premises solutions, tend to have needs for deeper IGA functionality than what the web-centric vendors typically provide. These prospects also tend to require customization and integration with legacy architected systems as well as a variety of directories and databases. This is forcing shallow-function, web-centric IDaaS vendors to add deeper functionality and integration capabilities to their roadmaps. Web-centric vendors have begun to develop these features, such as multilevel access approval workflow and access certification.

Microsoft made Azure Active Directory Premium generally available in May 2014. Since that time, Microsoft's sales organization has been very active in its customer base, and has been highly successful in selling its EMS, which includes Azure Active Directory Premium. Other web-centric IDaaS vendors are now repeatedly identifying Microsoft as the vendor that is "showing up" most often in competitive situations.

Conversely, some IDaaS vendors with deeper IAM functionality and integration capabilities tend toward implementations that are larger and more complex, and they do not have their offerings price-tuned for rapid handling of the down-market web-centric use cases. These vendors will need to provide a streamlined, rapidly deployable offering for these use cases if they wish to gain a piece of the SMB market.

Mobile Device Integration Continues to Evolve

Most IDaaS vendors support a portal-like interface on mobile devices for web applications that are under IDaaS management. IDaaS vendors began supporting customers' mobile apps by offering software development kits (SDKs). Customers can develop their apps using the IDaaS vendor's SDK, which will provide authentication to the IDaaS vendor's service. However, this is generally a proprietary approach that would require some rework, should the customer switch IDaaS vendors.

Centrify, and Okta provide an EMM capability integrated with the IDaaS. This allows for integrated device and identity service registration, account and application provisioning, and the use of device security posture and contextual data to support access enforcement actions at runtime. Microsoft's Intune is integrated with Azure Active Directory, but is not yet as tightly integrated as Centrify's and Okta's offerings. IBM has begun the integration of its CIS and its MaaS360 EMM. VMware AirWatch, which did not meet the inclusion criteria for this Magic Quadrant, has entered the IDaaS market with a workforce-centered offering that also integrates the VMware AirWatch EMM toolset.

Basic IAM functions continued their journey toward commoditization. SSO to web applications is a commodity, and basic IGA and analytics functions will take a bumpy and winding road to commoditization. User self-service access request and profile management, password reset, access approvals and account provisioning to web-centric targets, and canned and customized reporting are on the way to commoditization. More advanced IGA and analytics features will take longer, or will remain as differentiators for some vendors. Clients should expect overall downward pricing pressure in the market for the next three years.

On-Premises Replacement

Wholesale replacement of traditional on-premises IAM software stacks, which are serving multiple use cases for large enterprises, has been relatively rare. These on-premises implementations are long-standing, tend to be well-staffed and have been deployed to support legacy architected systems — not just web-architected and SaaS apps. Nevertheless, there are vendors that can support multiple use cases, have software with deep functionality that can be cloud-delivered and are capable of replacing legacy on-premises IAM tools. These vendors have been conservatively building businesses to do these things, and more customers are starting to use these vendors. However, we estimate that these kinds of deals represent only 5% to 10% of the overall market value.

Full-featured IDaaS implementations that support legacy applications can be deployed more rapidly by IDaaS vendors than by organizations buying and implementing software on their own. IDaaS can also remove some of the complexity of traditional software deployments. However, integration with legacy systems, multistep approval workflows, access certification and other IGA functions that are prevalent in mature IAM implementations still take time to plan, design and implement, and these planning and design functions add costs to implementations. Decisions to outsource complex IAM implementations aren't made easily.

Therefore, enterprises that are considering a "build" or an "extend," versus an "outsource," decision should focus on two key areas.

1. Inhibitors to successful on-premises IAM adoption, or issues with the current implementation that would potentially be alleviated or circumvented by the move to IDaaS, such as:

    Insufficient staffing levels or skills

    Organizational conflicts over duplicative IAM implementations obtained through mergers, acquisitions or independent organizational buying decisions

    Insufficient planning prior to tool selection and implementation

    Project scope creep

    Poor operational efficiency by IAM, resulting in too much time taken for IAM functions

    Poor operational effectiveness by IAM, resulting in audit findings for access violations

- With the exception of inappropriate staffing levels or skills, these inhibitors will not be automatically removed by switching to IDaaS. There often are root causes for these inhibitors that have nothing to do with the delivery model for IAM, and these issues must be addressed with solid IAM program management and governance. IDaaS simply may help to go around the problems, or alleviate some of them.

2. Total cost of ownership. There is no free lunch. Clients that judge IDaaS to be too expensive may not have done their homework in terms of understanding the full costs of managing on-premises IAM. These costs include:

    Fully burdened staff costs for implementers, operations staff members and a portion of the help desk personnel

    Software investment costs and ongoing maintenance

    Estimated patch and upgrade costs

    Infrastructure and operations for resilient implementations and business continuity

See "Use Business Drivers and Cost Analysis to Make IDaaS Versus On-Premises Software Delivery Model Choices" for more information.

Market Overview

This Magic Quadrant underscores a market that is in its adolescence and is still largely driven by web application use cases.

Competitive forces have increased due to large vendor presence in the market. Microsoft is beginning to have profound effects on the market in terms of competition and downward price pressure.

The IDaaS market originally was fueled by SMBs that used SaaS as their predominant application delivery model. Most of their applications already were in the cloud, and they preferred to buy rather than build infrastructure. In turn, SaaS applications became new identity silos, each with their own administration, authentication and event-logging capabilities.

IDaaS vendors can create connections one time to SaaS vendors for the purposes of authentication, SSO and account management (when SaaS vendors provide APIs to enable this). These connections can then be reused for new clients. This relieves the IDaaS customers of having to create these connections themselves. IDaaS vendors also can bridge to customers' on-premises identity and authentication services, and use data held or removed from there (such as directory group or organizational unit membership) to provision and deprovision accounts on SaaS targets. This automation saves customers the effort of manually provisioning and deprovisioning accounts, and also can help with avoiding orphaned and active accounts on SaaS that can leave enterprises vulnerable and paying for unused accounts.

In the past few years, vendors with the ability to broker all the functions between users and SaaS have become appealing to organizations of all sizes. Cloud security and data residency concerns, however, often are key factors in evaluating IDaaS vendors. The growth of the IDaaS market has been driven by the following factors:

The need to instill IAM disciplines for managing identities for SaaS applications

The need to gain faster time to value over traditional on-premises software

The desire to avoid IAM implementation failures

The desire to reduce IAM talent costs in design, implementation and support

Gartner estimates that the market size for multifunction IDaaS at year-end 2015 was just over $600 million. We estimate that 2016 revenue will be approximately $1 billion. Both estimates do not include revenue from vendors that provide single-function IDaaS offerings — for example, authentication-as-a-service vendors.

Over the past few years, web-centric IDaaS vendors have made solid gains at the lower ends of the market, supporting the employee-to-cloud use case. As these vendors have moved upmarket, they find that larger organizations tend to have IAM solutions in place, and have deeper IGA functionality needs than web-centric vendors can provide. These prospects also require integration with legacy architected systems. This is forcing shallow-function, web-centric IDaaS vendors to add deeper functionality and integration capabilities to their roadmaps.

Conversely, IDaaS vendors with deeper IAM functionality and integration capabilities tend toward larger, complex implementations, and do not have price-tuned offerings for rapid handling of web-centric use cases. These vendors will need to provide a streamlined, rapidly deployable offering for these use cases if they wish to gain a piece of the SMB market. Indeed, these bidirectional moves are starting to happen. By the end of 2017, we anticipate the fuzzy line between web-centric and full-featured offerings to get even fuzzier. Also, as greater portions of organizations' applications become web- or mobile-architected, we anticipate that a portion of the market previously reticent about using IDaaS as the only delivery model for IAM will begin to do so. We believe that this will affect mostly the midmarket (see "Predicts 2016: Identity and

Access Management"). Overall, by 2020, 40% of IAM purchases will use the IDaaS delivery model — up from less than 20% in 2016. Of those IDaaS implementations, Gartner believes that 40% will replace on-premises IAM implementations (rather than simply augment those implementations) — up from 10% in 2016.

The employee-to-cloud use case drove growth in the early IDaaS market, and it still predominates. B2C use cases have grown in importance as organizations look to replace a mixture of custom-developed IAM products and traditional on-premises IAM products. Some larger organizations also are "peeling off" the part of their IAM needs that are served by IDaaS, even when they may own IGA and access tools that could be extended to the cloud. For this use case, IDaaS is being viewed as a quick win, and sometimes as a way to standardize a solution for one part of the enterprise IAM problem space.

See the Context section above for a deeper analysis of market trends, a closer look at security and data residency concerns, and information on pricing.

Evidence

The following sources were used in the creation of this research:

Gartner client interactions

Phone interviews and online surveys for vendor-provided references

A comprehensive vendor survey that aligned with the evaluation criteria

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

FOR OFFICIAL USE ONLY

IDAM High-Level Evaluation

In response to the request of the Program Board to provide a rapid evaluation and recommendation of the available IDAM options available to iConnect. To be identified as a candidate for assessment, the solution needed to meet one of the following three criteria:

- Software already owned, or substantially owned by the Territory;
- Capability able to be acquired from another jurisdiction under a contract or other suitable instrument; and
- Able to be acquired on an as-a-Service basis via an existing Territory contract/license.

In addition, the solution must:

- Immediately meet the technical and integration needs of a minimum viable product and have the capability to meet more demanding needs over time;
- Be able to be implemented production ready in a relatively short timeframe (i.e. not require protracted procurement processes); and
- Not attract any significant technical or commercial implementation risk.

IDAM Options

The following six IDAM solutions were identified using the selection criteria set down:

Software already owned

- Sch 2.2(a)(x) - existing contract held by iConnect.
- Sch 2.2(a)(x) - existing software suite partially owned by ACT Revenue

Capability able to be acquired from another jurisdiction

- Sch 2.2(a)(x)
- Sch 2.2(a)(x)

As-a-Service from an existing supplier

- Sch 2.2(a)(x) - Cloud based service aligned with Shared Services ICT
- Salesforce Identity – Cloud based service aligned with the Wave 2 technology stack

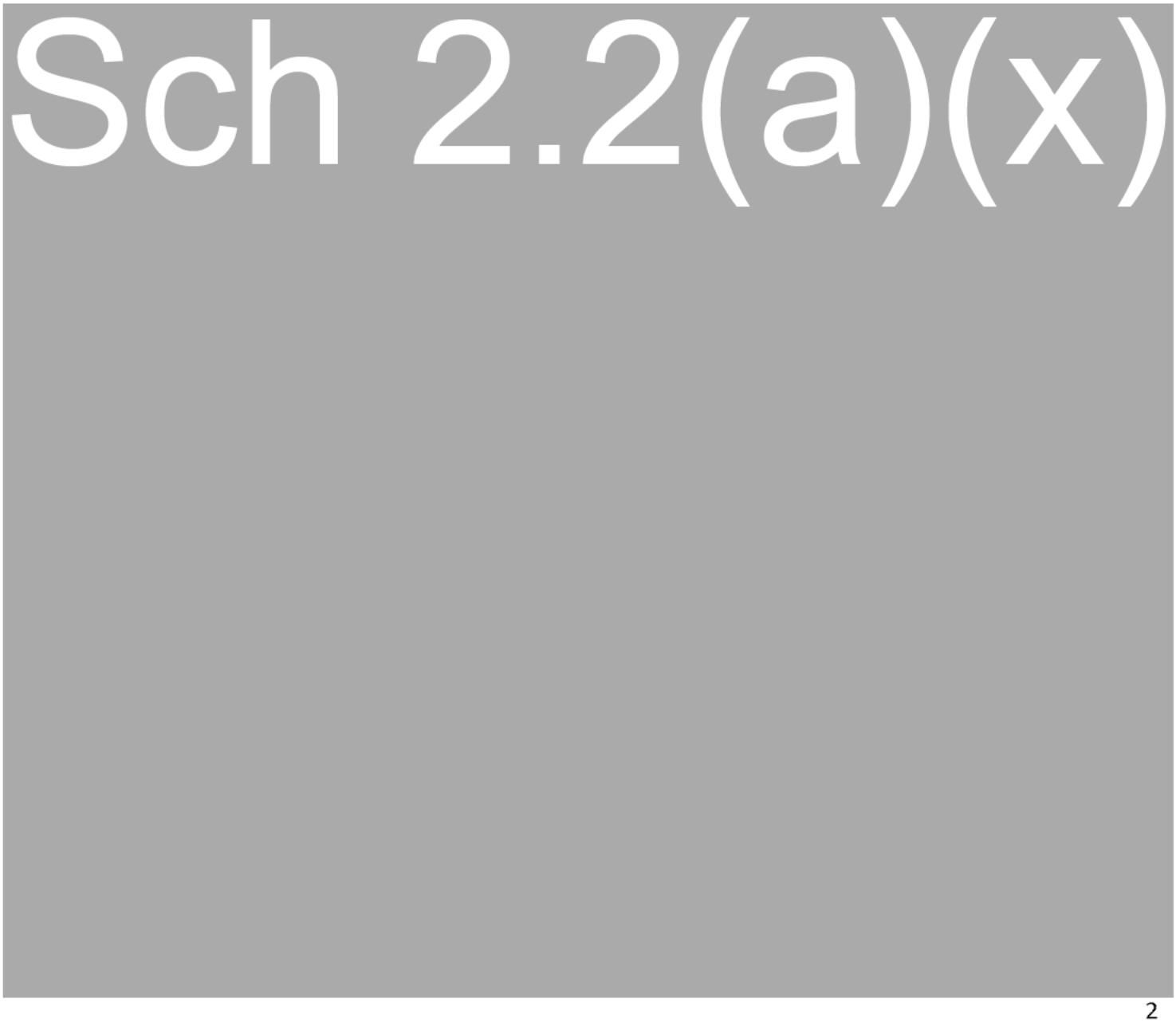
A potential IDAM offering from Sch 2.2(a)(x) was also considered but it was found that its acquisition would require and open tender process and so not meet the timeframe requirements.

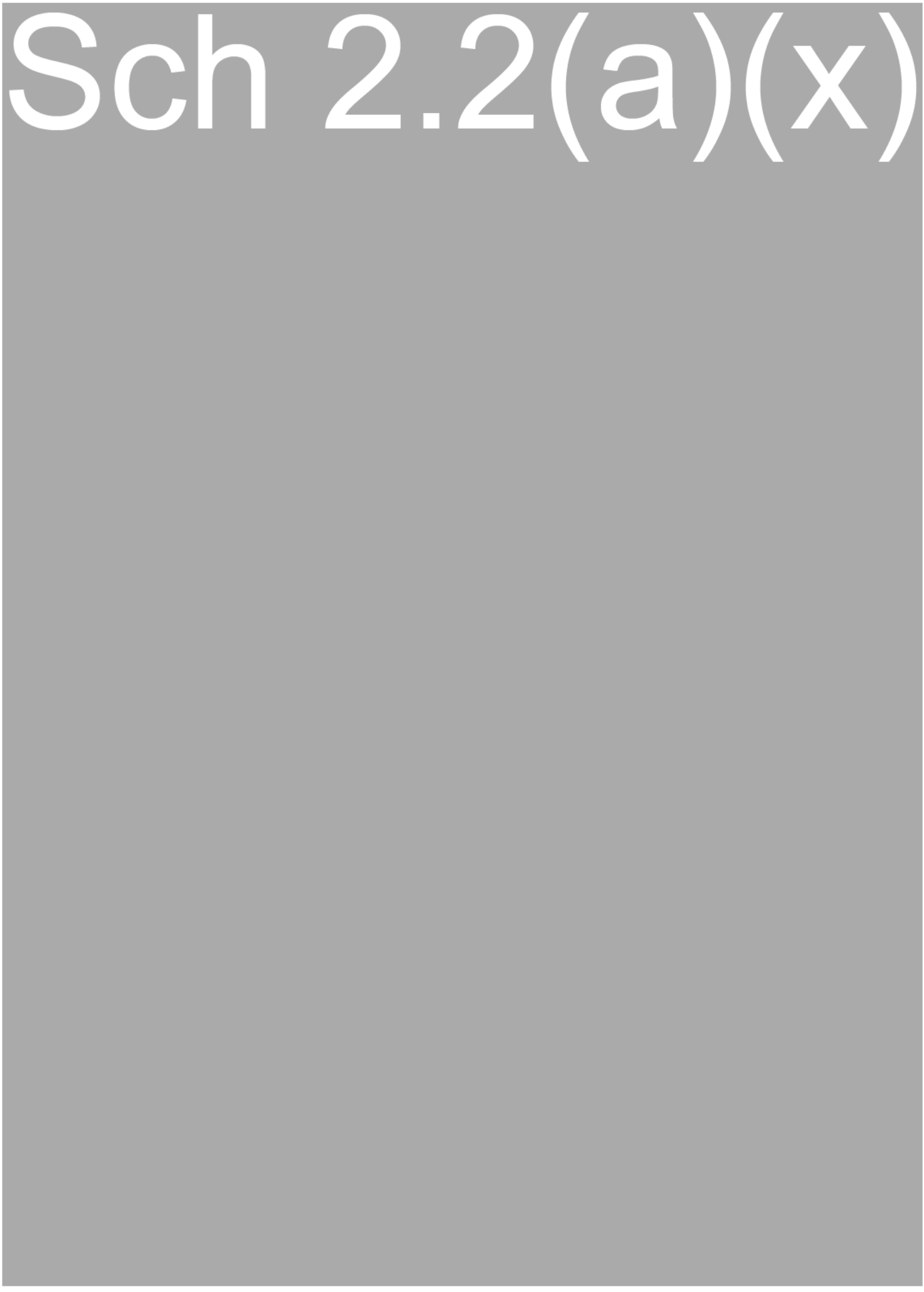
Assessment Criteria

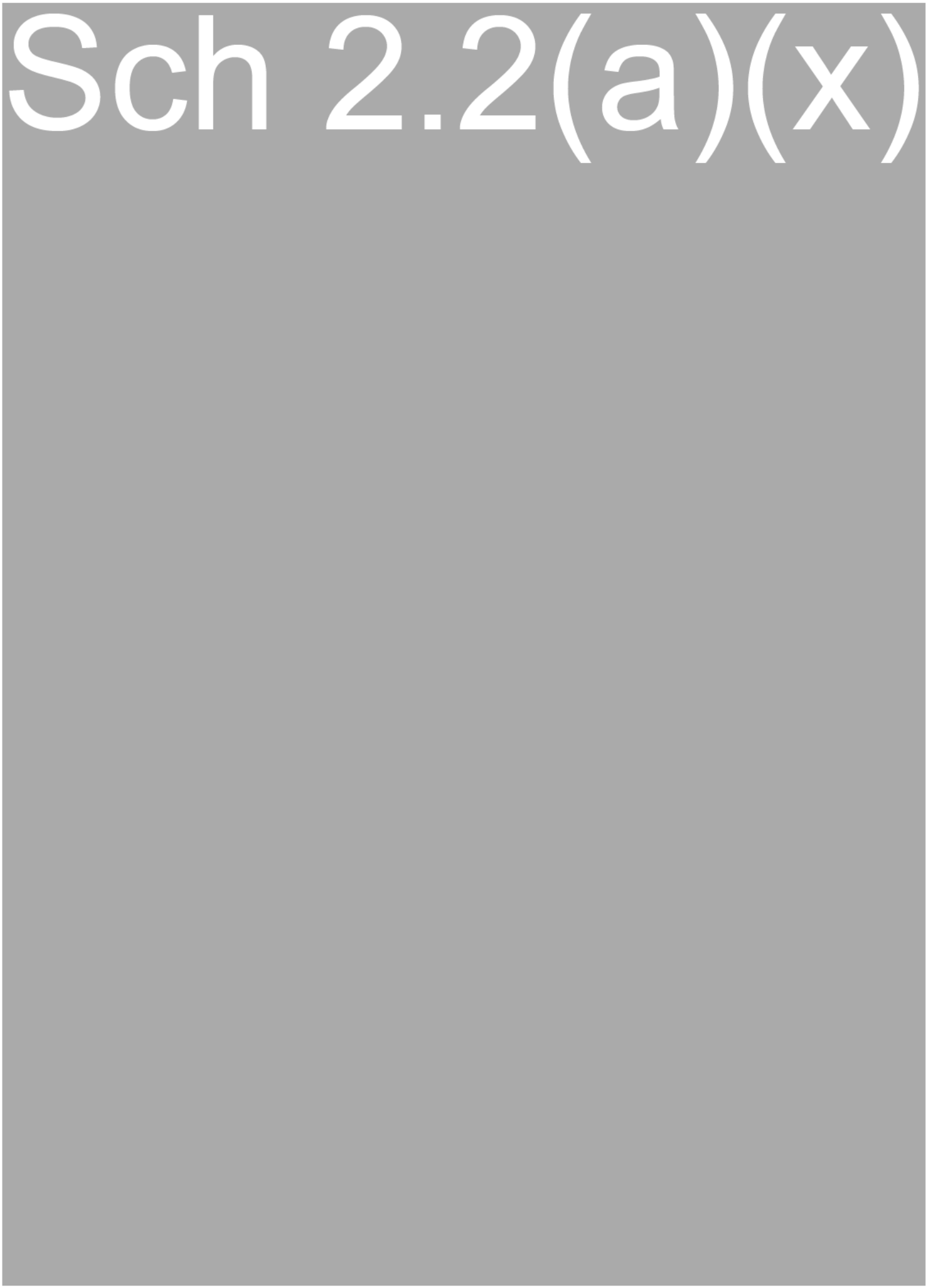
The following criteria was used to guide the recommendation. While the criteria are used to identify strengths or weaknesses of each solution, it should be noted that an exhaustive evaluation has not been performed against each product. This is due to several of the solutions not being available in the market place at the time of the original approach to market, or options now being available for evaluation from other jurisdictions.

Each of the six solutions were ranked from High to Low in each of the following categories:

- Maturity
- Available as a service
- Commercial risk to implement
- Technical risk to implement
- Completeness of solution
- Cost effectiveness
- Ease of acquisition




Sch 2.2(a)(x)


Sch 2.2(a)(x)

Sch 2.2(a)(x)

Sch 2.2(a)(x)

Candidate 6 – Salesforce Identity

Background

The Salesforce Identity (SFDCI) offering is a comprehensive cloud based identity management solution for customer facing web and mobile applications. SFDCI can be integrated with on-premise services such as Microsoft Active Directory also allowing integration with legacy applications.

SFDCI is used by a number of Australian state governments including the Victorian Department of Health and Human Services and the South Australian government.

SFDCI is ranked in the Visionary Quadrant of Gartner's current Identity-as-a-Service Magic Quadrant. SFDCI is most commonly implemented as part of utilisation of the Salesforce PaaS platform; it can be utilised as a standalone IDAM without the need for the utilisation of other Salesforce applications however this is a uncommon utilisation case.

SFDCI is procured as Platform-as-a-Service (PaaS) with monthly costs based on the number of user accounts held, or by consumption. Options are available for bundling of SFDCI should other Salesforce applications be subscribed to. As part of the Wave 2 implementation the ACT Government has a license to utilise the SFDCI. This option was investigated due to utilisation of the Salesforce application in digitalising the Wave 2 process, and given the role Salesforce plays in the SNSW technology stack, where it delivers much of the CX.

Findings

- SFDCI is a mature offering originally launched in 2013.
- SFDCI is ranked by Gartner as a Visionary.
- The predominate use case of SFDCI is business to customer (B2C) or government to citizen (G2C).
- iConnect is delivering Wave 2 using the Salesforce application platform, which is natively integrated with SFDCI.
- Native integration between Salesforce and SFDCI enable rapid prototyping and simplified deployment.
- Only limited deployments of SFDCI have been achieved without also adopting the Salesforce platform.
- SFDCI pricing aligns with iConnect requirements for consumption based pricing.
- The Salesforce partner ecosystem provides a competitive marketplace for the supply of specialised services within Australia.
- Shared Services ICT will develop their own in-house skills with Azure AD which would de-risk iConnect adopting of B2C.
- The existing Salesforce master agreement does not allow for additional licenses to be acquired without an approach to market.

Assessment

Maturity	High. The SFDCI solution was released over three years ago, and has been continually updated with new capabilities since.
As a service	High. SFDCI is a PaaS platform.
Commercial Risk	Medium. An existing contract exists between iConnect and Salesforce; a revised contract has been negotiated to incorporate compliance with the Territory Privacy Principals.
Technical Risk	Medium. While meeting many of the requirements of iConnect, the ease of technical integration is best achieved when the CX layer is also hosted by Salesforce.

Completeness	Medium. SFDCI is recognised by analysts as a leader in the field of IDAM solutions. However, it is not clear that the SFDCI will be sufficiently capable and extensible to meet iConnect's requirements.
Cost Effectiveness	High. The SFDCI pricing available to iConnect under existing contracts is financially viable.
Acquisition Method	Medium. An existing licensing agreement with Salesforce is in place however the ability to expand beyond the current entitlements would require a new approach to market.

Assessment

The below matrix summarises the assessment results across the six evaluated solutions.

	Sch 2.2(a)(x)					
Maturity	Low	Low	High	Medium	Low	High
As a service	High	High	High	High	High	High
Commercial Risk	Medium	Unknown	Medium	Medium	Low	Medium
Technical Risk	Medium	High	Low	Unknown	Medium	Medium
Completeness	Low	Unknown	High	Unknown	Low	Medium
Cost Effectiveness	Medium	Low	High	Unknown	High	High
Acquisition Method	High	Unknown	High	High	High	Medium
Rating	**Not Suitable**	**Not Suitable**	**Highly Suitable**	**Not Suitable**	**Partially Suitable**	**Suitable**

Based on the assessment above, there are is a clear standout option available to iConnect in the Sch 2.2(a)(x) IDAM offering. The many years of developing their IP through their own customer development processes will accelerate iConnect's own delivery. Should Sch 2.2(a)(x) be able to confirm that the proposal as supplied includes the Identity profile and service profile management, then the advantages of adopting this offering are significant and should drive decision making over and above the underlying technology components.

Appendix E

Program Board 13 June – Minutes

Appendix E: Minutes of Program Board meeting 13.6.17

Out of scope

ACT Government
Chief Minister, Treasury and Economic Development

MINUTES

iConnect Program Board Meeting

Tuesday 13 June 2017, 2:30pm-4:00pm – Level 5 Conference Room, Nara Centre

1. Record of attendance

Attendance	Jon Cumming, Chief Digital Officer (Chair), CMTEDD	Dave Peffer, DDG, Access Canberra, CMTEDD
	David Colussi, Director, Digital Experience (Program owner), CMTEDD	Kim Salisbury, ACT Revenue Commissioner, CMTEDD
	Gary Spencer, A/g Director, Finance and Operations, EPSD Amy Phillips, A/g Director, Strategic Business and Programmes, SSICT	Mark Huxley, Chief Information Officer, Education
Invited	Sim Prescott, iConnect Program Manager, CMTEDD	Tracey Smith, Manager, iConnect Organisational Governance
	Joel Madden, Director, DSGC Support Executive	
Apologies	Michelle Narracott, Executive Director Strategy, Innovation and Customer Experience, TCCS	Anita Perkins, Director, Communications, CMTEDD
	Meg Brighton, DDG, Education Directorate	Gary Davis, Executive Director SSICT, CMTEDD
		Jack Radik, Independent Quality Assurance Officer (IQA)

Sch 2.2(a)(x)

Out of scope

The Program Board agreed the iConnect program pursues alternative pathway of CX and CIDAM via Salesforce; and that the program seek approval to exemption from public tender for a single select procurement of Salesforce. The Program Board adopted option 3, as indicated above, to:

- Retain a strategic relationship with Sch 2.2(a)(x)
- Do not pursue use of the Sch 2.2(a)(x) platform
- Progress Salesforce to Beta
- Prepare and consult on single select to cover three years (assumes a one year procurement lead in time at year 2 mark)

Out of scope

6. Next meeting

Next Meeting: 3 August 2017

Appendix H

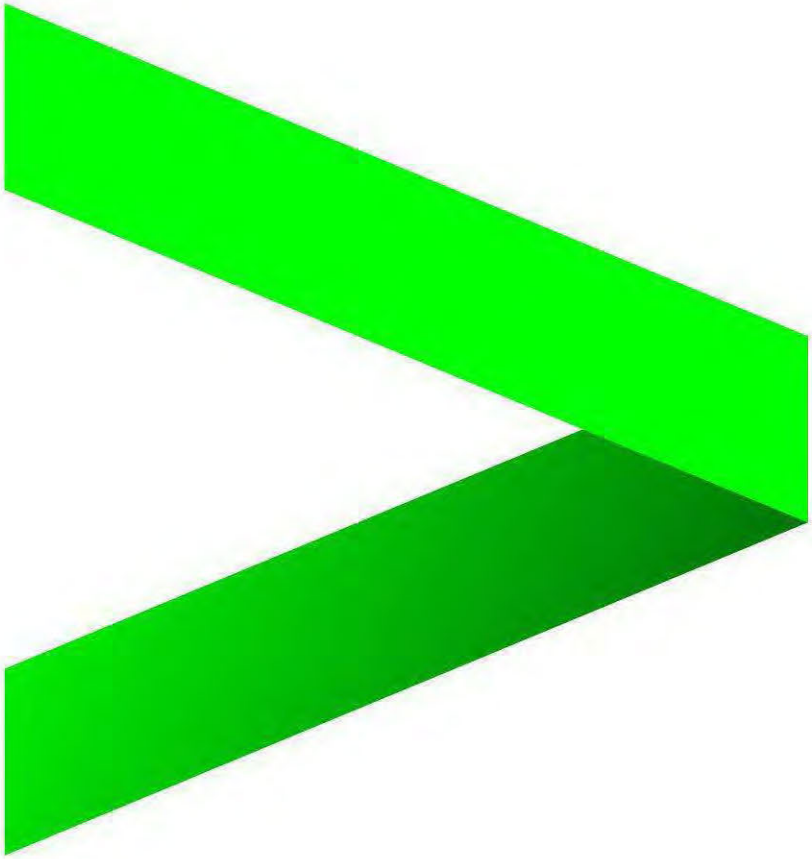
Salesforce Platform Selection Review, Accenture

ACT Government

iConnect Digital Account Platform

Salesforce Platform Review

28 July 2017



accenturetechnology

EXECUTIVE SUMMARY

The ACT Government Digital Strategy seeks to "create the impetus and architecture for platform renovation". The guiding principles applicable to iConnect are:

1. Start with the customer relationship
2. Digital Services – Mobile Devices
3. Cloud is the service platform ("Software as a Service rather than bespoke applications")

iConnect is a key delivery program for the Digital Strategy and is required to establish an extensible digital account for citizen identity that enables Directorate service delivery. Accenture has been engaged to complete a high level review of the suitability of Salesforce to deliver against the requirements of the iConnect Program; specifically:

1. Digital identity platform
2. SSO capability
3. Enterprise grade security
4. Extensibility
5. Future proof capability set

Accenture has assessed the requirements of the iConnect Program and found that Salesforce is a suitable platform to deliver the intended services. The following report details the alignment between the Program elements and the Salesforce capabilities intended for execution.

THE ACCENTURE REVIEW TEAM

Steven Herod – Salesforce Certified Technical Architect

Steven Herod is an experienced Enterprise Architect with a specialization the Salesforce platform. He has architected, implemented and reviewed numerous complex Salesforce implementations across Retail, Insurance, Government, Banking, Manufacturing, Media and Health.

Steven holds 19 separate Salesforce.com Certifications including Certified Technical Architect for which he has also acted as a Judge and contributed Salesforce Architect Academy exam curriculum.

Rohan Bentley – Salesforce Government & Health Lead

Rohan leads the Cloud First team for all SaaS related projects in the Government and Health sectors across Australia. Rohan has over 20 years experience in the IT industry with 15 focused on CRM across multiple industries.

Rohan has focused on Salesforce since 2011 having led major projects here in Australia as well as multi-national projects.

ASSESSMENT INPUTS

MEETING
Assessment was made based on a meeting with iConnect staff on 24 July 2017

DOCUMENTATION
Review based on Presentation entitled 'Digital Account Platform v1.2.pdf'

NO SYSTEM REIVEW
Inspection of the Salesforce instances including security and data model was not undertaken due to the limited timeframe provided for the review.

THE NUMBERS
Volumetric data was provided by iConnect staff as detailed on Slide 6.

Based on the available inputs, Salesforce can support the intended use cases. The following slides provide further detail to support this assessment.

ASSESSMENT RESULTS

PLATFORM

- Salesforce will scale to the size required by iConnect
- Salesforce provides a suitable framework and security model
- Salesforce can meet the solution requirements as a citizen engagement and identity platform

SCALABILITY

- Salesforce can scale to the volumes described for identity management
- Salesforce is not suitable for the volume of data required for public transport tap on/tap off transactions

SECURITY

- The Salesforce security model is capable of meeting the requirements of this program
- The use of standard salesforce security is strongly encouraged, noting that Salesforce communities are not currently capable of 2 factor authentication without customisation.

IDENTITY

- The storage of identity information in Salesforce could be undertaken if appropriate obfuscation / encryption approaches are considered
- Appropriate procedures and policies should be in place to manage citizen identity

OUR UNDERSTANING OF REQUIREMENTS

1. iConnect will provide a Digital Identity platform for ACT (and near by NSW) residents.
   - Salesforce is a suitable solution for delivering a Digital Identity Platform.
   - The use case is similar to the existing ServiceNSW solution also based on the Salesforce platform
2. SSO capability will allow Salesforce to connect with the existing Oracle Access Canberra database
   - Salesforce has suitable SSO Capability (SAML2.0 and Oauth) for this program.
3. The CDO wishes to ensure that the Salesforce platform is an enterprise grade capability that can support these requirements for a period of at least three years. The security aspects are being assessed through an IRAP assessor that has been engaged.
   - A strong security audit is recommended for the current and all future phases.

A detailed response to each requirement is available in the appendix

OUR UNDERSTANING OF REQUIREMENTS

4. iConnect Outbound messaging (SMS/Email) will be managed via Marketing Cloud
   - Salesforce provides suitable functionality to deliver the Outbound Messaging requirements of the iConnect Program.
5. Customer Portal will utilise Extendable forms and CX (Using Communities and Vlocity)
   - Salesforce with Vlocity provides suitable capability in extendable forms and CX
6. Payment Services will be via a Westpac gateway
   - Westpac payment gateway connected to Salesforce is a common use case and is consistent with industry standards.
7. Native Mobile Application will be developed
   - The development of native mobile applications for Salesforce is consistent with industry best practice.

A detailed response to each requirement is available in the appendix

OUR UNDERSTANDING VOLUMETRIC DATA

Personalised Digital Services to be provided include:

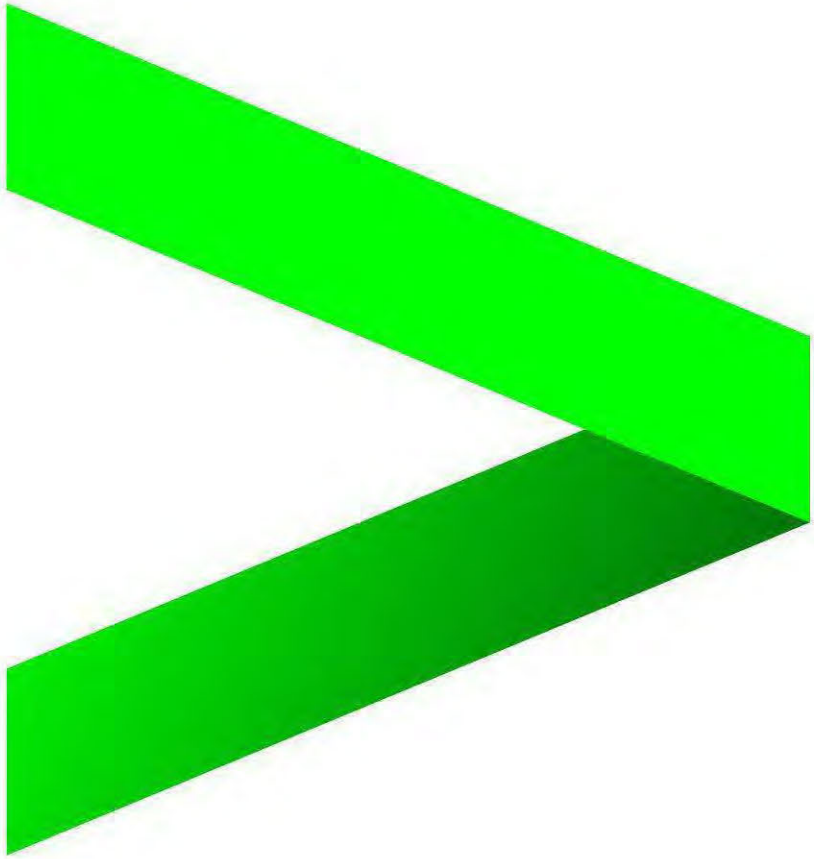
1. Customer Logins
   - The forecast logins of customers into the Digital Account is forecast up to 250,000 logins in Year 3.
   - This is well within the capabilities of the Salesforce platform.
2. Outbound Messaging Usage
   - It is expected that outbound communications usage will be up to 5,000,000 messages in Year 3.
   - This is well within the capabilities of the Salesforce platform.
   - Outbound Communications are within scale. Care should be taken to use appropriate patterns and external middleware may be appropriate.
3. ACT Government Employee Usage
   - The expected usage of Salesforce services by ACT Government employees is estimated as 250 Service Cloud Users and 10,000 Community Users in Year 3.
   - The number of internal users is small/moderate range for Salesforce and well within the capabilities of the platform.
   - The number of Community users is in the moderate range and well within the capabilities of the platform.

ACT Government

Appendix

Salesforce Platform Review

1. General Recommendations
2. Technical Recommendations
3. Detailed Response to Requirements



accenture technology

GENERAL RECOMMENDATIONS

1. Configure Not Code
   - Salesforce configuration should be used prior to bespoke development wherever practical.
2. Integrations
   - Identify and analyse all legacy application interactions as early as possible.
   - Consider using data virtualisation (OData) where possible.
3. Dev Ops
   - A stringent and scaled DevOps capability is recommended to ensure successful delivery and deployment of the platform.
   - The environment management solutions approaches will need uplift with the programme expands.
4. Delivery Team & Approach
   - Using a small team of highly skilled resources onsite integrated with the broader program team is recommended.
   - Take advantage of offshore development where practical, understanding the limitations regarding data access outside of Australia.
   - A Salesforce Certified Technical Architect should be engaged on a project of this size.
   - When scaling up delivery it is critical to follow a well standardised and managed strategy and approach to ensure consistency and efficient development.
5. Delivery Approach
   - When scaling up delivery in a programme this size, it is critical to follow a well standardised and managed strategy and approach that is able to support its implementation across the ACT Government to ensure consistency and efficient development.
   - Large projects involving multiple stakeholder groups (in this case Directorates) can have fragmentation of design and standards. This lack of standardisation can and inhibit the ability to achieve economies of scale.

TECHNICAL RECOMMENDATIONS

1. Standard Encryption & Security
   - Use standard Salesforce Encryption add Security capability whenever possible.
   - It is noted that the lack of Two Factor Authentication on Communities has required custom development.
   - Platform encryption is not a benign function – it requires continual architectural review.
2. Middleware
   - Consider a middleware solution between Salesforce and other integrated systems, particularly as the overall solution becomes broader and more complex.
   - Middleware should be used for any high volume transaction based integrations (eg. Bus ticket tap on/off).
3. Execution Governors & Limits
   - Salesforce's multi-tenant Execution Governors and Limits should be reviewed prior to any significant development that involves large volumes of data and/or transactions.
4. Data Governance
   - A documented and managed Canonical data model – covering the identity platform and the overall solution – is recommended.
   - Implementation of a Data Loss Prevention Strategy is recommended – Salesforce Shield has capability that supports this.
   - Implementation of a full backup strategy is recommended.
5. Multiple Org Strategy
   - A Multiple Org strategy is being considered – further analysis is necessary to understand the appropriate breakdown of functionality between each Org - a Multiple Org strategy may not be the best solution for iConnect.

DETAILED RESPONSE TO REQUIREMENTS

1. iConnect will provide a Digital Identity platform for ACT (and near by NSW) residents. The current Communities implementation is based on Service Cloud using encryption (Shield Platform Encryption) for Personally Identifiable Information (PII)
   - The use of Customer Community is a valid use case consistent with the products functionality.
   - The use case is similar to the existing ServiceNSW solution also based on the Salesforce platform. It should be noted that the iConnect approach includes enhanced identity management which is beyond the scope of the ServiceNSW system.
2. SSO capability (based on SAML2.0 and OAuth) (standard platform capability and demonstrated with SSO to existing Oracle Access Canberra database)
   - The use of SAML & OAuth federated authentication is a valid and should be continued.
   - Currently, Salesforce does not natively support two-factor authentication for communities. To provide this functionality, a combination of additional configuration and custom development has been implemented. This custom functionality should be rolled back to standard functionality when the capability becomes available (timeline is currently unknown).
3. The CDO wishes to ensure that the Salesforce platform is an enterprise grade capability that can support these requirements for a period of at least three years. The security aspects are being assessed through an IRAP assessor that has been engaged.
   - A strong security audit is recommended for the current and all future phases.
   - It is recommended that there are documented practices and procedures for the handling of personally identifiable information.

DETAILED RESPONSE TO REQUIREMENTS

Personalised Digital Services to be provided include (via Communities, Marketing Cloud and Vlocity):

4. Outbound messaging (SMS/Email) is managed via Marketing Cloud
   - The use of Marketing Cloud (Exact Target) is a valid use case consistent with the products functionality.
   - Effective use of the Marketing Cloud capabilities ensuring high open rates and greater connection to the target audience requires dynamic content, AB testing, personas, segmentation, multilingual content and journeys.
   - Net Promoter Score survey could be provided by Marketing Cloud's Survey Builder.
   - Chatbot functionality can be integrated with Marketing Cloud and Service Cloud to reduce call rates.
5. Extendable forms and CX (Using Communities and Vlocity)
   - The use of Vlocity Omniscripts capability exposed via a Salesforce Community is a valid use case consistent with the products functionality.
   - Vlocity's internal facing omniscripts and console functionality can be used to streamline the support agent workload.
   - Vlocity is currently used by a number of Cities in the USA as well as large insurance agencies.
6. Payment Services (utilising existing Westpac gateway. Salesforce will not perform reconciliation)
   - Westpac payment gateway connected to Salesforce is a common use case and is consistent with industry standards.
7. Mobile Application (leverages Salesforce mobile SDK with native app, first priority is iOS)
   - The development of native mobile applications using the Salesforce SDK is consistent with industry best practice.
   - The use of Salesforce1 capability for iConnect is not recommended.

ACT Government
Chief Minister, Treasury and Economic Development

GOVERNMENT PROCUREMENT BOARD

STRATEGIC REVIEW SUBMISSION

SUBMISSION OVERVIEW	
Name of Procurement	iConnect program – Customer Identity Management service
Purpose	This Submission informs the GPB of the proposed procurement strategy to: • deliver a Citizen Identity and Access Management (CIDAM) capability using Salesforce, and • re-test the market for CIDAM services after 2 years and within 3 years, in the expectation that it will have matured.
Estimated value ($)	*Single select component: $990k inc GST over 3 years *formal RFI due from Salesforce week of 26 June* *Market-tested/panel component: per iConnect development budget*
Procurement Risk	Low.

SUBMISSION DETAILS	
Scope	SUMMARY: 1. The original procurement strategy of 14 November 2014 resulted in a contract with Sch 2.2(a)(xi) for the CX technology platform and Sch 2.2(a)(xi) for the CIDAM PING technology platform. 2. The result was an arrangement with poor vendor support, oversold technologies and under-delivered 'out of the box' solutions. The contracts contained minimal delivery compliance metrics. 3. A formal review resulted in a pivot point creating two concurrent streams of work. 4. The first involved investigating the potential to partner with ServiceNSW to purchase their customer service solution "as-a-service". 5. The result, despite significant goodwill and effort, was a number of insurmountable challenges remained including the completeness of the solution, unclear pricing and legal barriers. 6. The second stream of work involved exploring the capability of the Salesforce technology used by ServiceNSW, through a small-scale procurement. 7. The result has been successful proofs of concept and pilots using Salesforce cloud platforms to develop, iterate, test and deploy solutions quickly. 8. Comparing the two workstreams it was found that with the reduces scope of the Sch 2.2(a)(xi) capability, the Salesforce component was providing all but one aspect of the total required solution – this remaining piece being

the core identity function that was easily to include in the Salesforce application.

9. The iConnect Program Board has assessed the Salesforce solution as the best option currently available and has endorsed its adoption to meet the CIDAM needs of the Territory, supporting the bid to obtain approval for a single select procurement.
10. The iConnect Program Board has further determined that the CIDAM market should be re-tested within 3 years, to take advantage of expected improved market maturity. In practical terms this entails approaching the market after 2 years at which point it is expected that other vendors, as well as the DTA GovPass product, should be well established.
11. It is recognised that the Head of Service will require a comprehensive and compelling case to support the single select case.

DETAILED DISCUSSION:

iConnect is a four year program that was funded as part of the 2014-15 ACT Budget.

In 2016-17 the Program's key objective is to establish Whole of Government Citizen Identity and Access Management (CIDAM) capability to enable single sign-on (SSO) and identity verification for citizens accessing ACT Government services.

The ACT Government's Digital Account, known as MyAccount, will offer citizens personalised services through the digital channel. It will deliver directorates the ability to interact with customers via a secure, authenticated and trusted account, and option to offer more services via the digital channel. It will also replace the identity component of Access Canberra's existing online customer account.

The iConnect program is delivering on the ACT Government Digital Strategy 2016-2019, notably through the technology and business transformation to offer citizens improved access to government services, the ability to 'tell government once', and to opt in to share their data for a better service experience.

The iConnect program is an agile program in business and technology methodology, meaning that it has consistently ensured that solutions and technology platforms are rigorously tried and tested before release to the public. The program has arrived at the decision point outlined in this paper following three extensive technology pilots.

Sch 2.2(a)(x)

A decision to pivot from the technology was made on the basis that the vendor support was poor, the technologies were 'oversold' and under delivered on 'out of box' and that the model of one integrator and two technologies did not provide reasonable assurance of success.

The iConnect Program Board initiated a full program review in September 2016. Execution of the review provided an independent assessment on the program's

status and direction and a number of recommendations that informed a redefined delivery plan for the iConnect program. The redefined delivery plan was endorsed by the iConnect Program Board on 2 February 2017 and is focused around the sourcing, configuration and releasing to production the core enabling ICT platforms.

A Software as a Service platform, Salesforce, was chosen for the next pilot as it is one of the few mature platform options and it also aligned to the Sch 2.2(a)(x) technology – (supporting that workstream as below). The iConnect team developed a solution for the organisational and customer management of parking infringements. This pilot produced the service design capability for organisational transformation, an exemplar roadmap to address the challenges in progressing from the current status of service delivery using online, office processing and databases to an end to end digital experience.

The pilot also proved the use of Software as a Service cloud platforms to develop quickly, to iterate and test and re-deploy solutions and highlighted the architecture required to connect cloud technologies to traditional systems of record.

Based on the success of the Parking Infringements pilot and the direction given by the board the iConnect program took the user feedback, technical architecture and design frameworks from the two pilots and focused on an ACT Government Digital Account using Salesforce whilst ensuring other Software as a Service technologies are able to be adopted where appropriate, cost effective and viable.

The two pilot programs Sch 2.2(a)(x) investigations and market research for the digital delivery of services very accurately defined the need for a secure, user friendly and inter-operable Customer Identity Management platform. This platform is an essential foundation for personalised services through digital channels.

Adopting agile, low cost and iterative development cycles the Salesforce CiDAM has proven a capability for the government to connect customers to all Directorate systems and provide a single entry point with authenticated customer credentials that can in the future can be matched with customer data for more personalised and streamlined service delivery.

The Board has assessed the Salesforce software as a service (SaaS) solution as the best option currently available. This is also supported by research from Ovum. The program board has therefore endorsed its adoption to meet the CIDAM needs

	of the Territory and the submission for a single select to effect an outcome in the medium term. The Board has determined that the CIDAM market should be re-tested after 2 years to check against a maturing technology market – requiring a 3 year single select.
Strategic Vision	The alignment of the iConnect program with the strategic vision of the directorate and ACT Government has already been established. This procurement will advance the achievement of iConnect's strategic objectives, in close alignment with the ACT Government Digital Strategy 2016-2019 ('the Strategy'). In particular it reflects the three core principles of the Strategy: • building digital foundations • delivering digital services, and • providing a platform for the growth of the digital economy in the ACT. It also strongly reflects the principles in the Strategy to: • prefer Cloud as the service platform • ensure the privacy and data security for the users of the service • procure responsively and achieve value for money.

Objectives	To procure two components and services which in combination provide a Customer Identity Management service for the ACT, as follows: **Component 1: Salesforce licensing (Single Select)** iConnect intends to licence sufficient Salesforce capability and capacity to satisfy CIDAM requirements for up to three years. Salesforce will deliver the CIDAM and customer experience (CX) components of the ACT Government's MyAccount CIDAM service. **Component 2: Salesforce Development & Support Services (Market-tested/panel)** Development and support activities required to (i) design, develop and deliver the CIDAM and CX capabilities through Salesforce; (ii) provision of support and maintenance services required to ensure that the Territory's Salesforce services are available, secure and operational; (iii) design and advisory services to further leverage the platform to deliver additional CIDAM capabilities.
Imperatives	Key dates for this procurement are: **Date** | **Activity** Mid July 2017 | Production system available to Directorate customers
Existing Territory arrangement	There is no existing Territory whole-of-government (WhoG) arrangement.
Procurement Strategy Options	**Options for component 1: Salesforce licensing (Single Select)** Given the direction from the iConnect Program Board to deliver the initial CIDAM in Salesforce, the only option for this procurement is to seek an exemption from open tender to procure the required service as a single select.

	Options for component 2: Salesforce Development & Support Services (Market-tested/panel) There is a market for development and support services for Salesforce. Options for procurement include: • utilisation of the DTA Digital Marketplace • utilisation of the (Australian Government) Whole of Government Cloud Services Panel • open or select tender The Small Business Innovation Program (SBIP) was considered but there is no known/accredited capability at this time.
Preferred Procurement Strategy	As noted, for component 1 of the procurement, single select is the only – and therefore the preferred procurement strategy. With respect to component 2, the ongoing SI requirements will be dictated by Directorate onboarding timing and requirements, and controlled by the program board governance processes. The preferred approach is an open RFQ or open RFT as required. Consideration will be given to selecting a supplier that will demonstrate a commitment to building a local presence – either directly or in partnership with a local company.
Consultation	Extensive consultation has demonstrated that: • a number of business areas across the ACT Government require a CIDAM service, which the iConnect solution will provide according to an industry standard specification • the resultant arrangement will be a new whole-of-government arrangement in that it will provide a CIDAM service available for all ACT Government business systems that require such a service • If this procurement were not to proceed and the program paused, individual directorates wold need to build their own individual capability creating a re-integration technical debt. • this is not a 'joint proposal' (e.g. one or more directorates).
Contract Management Strategy	The contract for the licence of the CIDAM through Salesforce will be a variation on the Salesforce Master Subscription Agreement. The variations have been negotiated with Salesforce based on ACT Government Solicitor Office (GSO) input to ensure compliance with Territory legislation including the *Privacy Act 1988 (Cth)* and the *Information Privacy Act 2014 (ACT)*. It is expected that the contract for the Salesforce Development & Support services will be a standard ACT Government services contract. Contracts will be managed initially by iConnect and transitioned to existing BAU units prior to the conclusion of the program. Contracts will have service levels including service availability, performance, incident response and resolution, allowing effective risk management by iConnect of these aspects of the service. Where appropriate, contracts will have indemnity and liability provisions that protect the Territory in the event of incidents related to privacy and security, mitigating the risk to the Territory of these aspects of the service. The contracts will include termination and

	transition out provisions ensuring the Territory will be able to ensure continuity of service in the event it changes CIDAM platforms.

PROJECT DETAILS	
Project Owner	David Colussi, Director, Digital Experience
Section / Division	iConnect, Office of the Chief Digital Officer
Stakeholder(s)	

Stakeholder	**Proposed role(s)**
David Colussi, Director Digital Experience	Contract Manager/Financial delegate
Jon Cumming, Chief Digital Officer	Procurement delegate, Chair of Program Board
Dave Peffer, DDG, Access Canberra, CMTEDD	iConnect Program Board Member
Meg Brighton, DDG, Education Directorate	iConnect Program Board Member
Kim Salisbury, ACT Revenue Commissioner, CMTEDD	iConnect Program Board Member
Gary Davis, Executive Director, SSICT, CMTEDD	iConnect Program Board Member
Gary Spencer, A/g Director, Finance and Operational Services, EPSD	iConnect Program Board Member
Michelle Narracott, Executive Director Strategy, Innovation and Customer Experience, TCCS	iConnect Program Board Member
Anita Perkins, Director, Communications, CMTEDD	iConnect Program Board Member

Other responsible officer(s)

Procurement Officer	Paul Treloar
Other Officers	Tracey Gower

RELEVANT DOCUMENTS (ATTACHED)	
Supporting Document(s)	**Attachment A:** Risk Identification

ICT PROCUREMENT OPTIONS (DELETE TABLE IF NOT APPLICABLE)	
Software Licensing	Salesforce licences will be included.
Cloud Services	The Cloud service proposed is SaaS.
Cloud Service Provider	The Cloud Service Provider will be Salesforce.
Cloud Data Issues	The Customer Identity Management service delivered by the iConnect program will entail personal information being collected, transmitted, stored, used and disclosed in a Cloud environment. The personal information is classified as UNCLASSIFIED DLM 'SENSITIVE'. The GSO are finalising a privacy policy and terms of use to seek citizen consent around the handling of their personal information in the cloud.