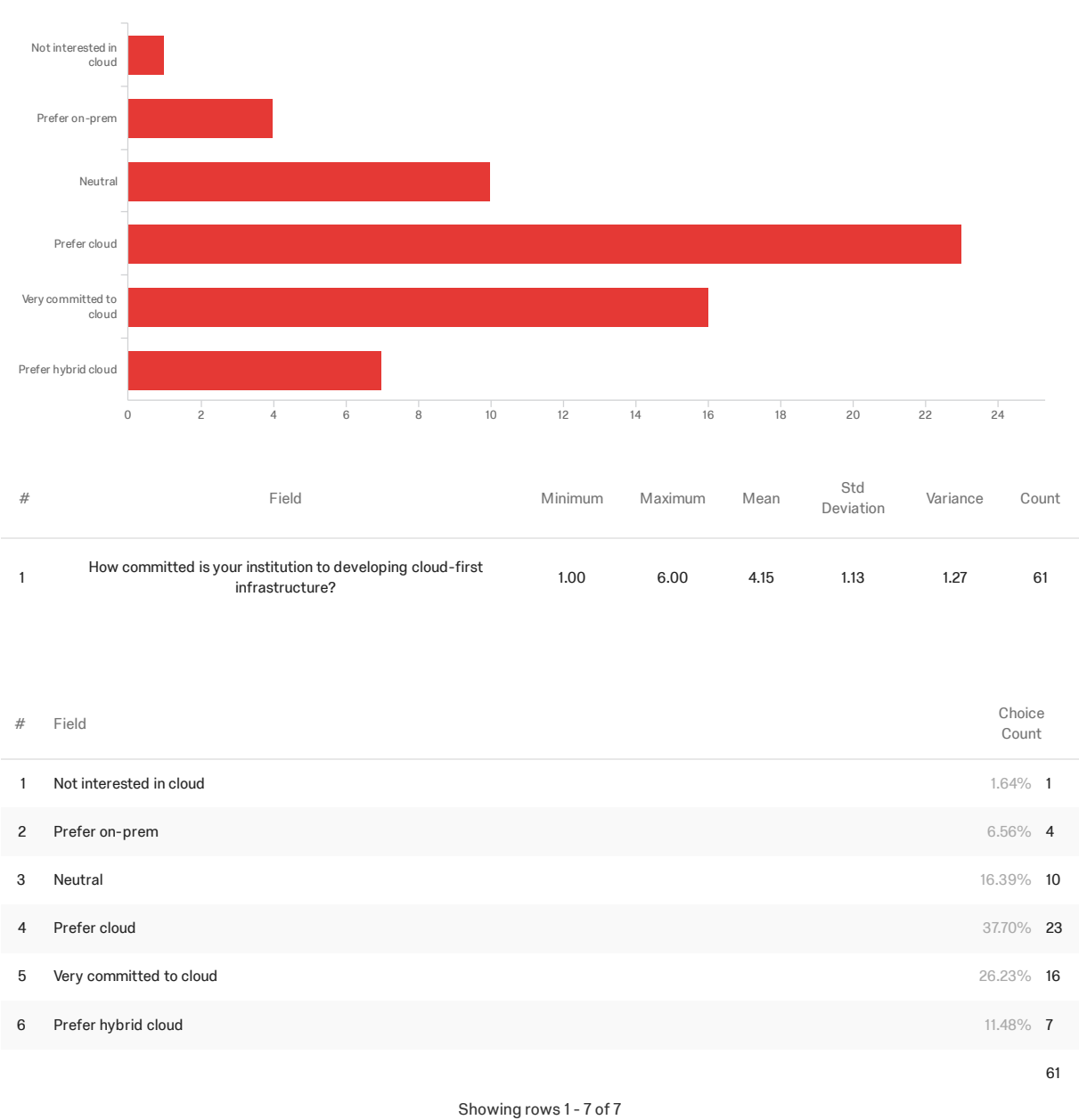


Q3 - How committed is your institution to developing cloud-first infrastructure?



Q4 - What does your institution use for single sign-on (SSO)?

What does your institution use for single sign-on (SSO)?

JASIG CAS, SimpleSAML

Ethos Identity Server

Acceptto

CAS, Shibboleth, Google SAML

shibboleth

Shibboleth/LDAP/CAS

Azure AD and ADFS (on-premises)

Shibboleth

Portal Guard

ADFS, Shibboleth, CAS (trying to reduce)

Microsoft ADFS

ForgeRock OpenAM

Shibboleth, ADFS

Fischer International SSO portal

ADFS currently, but are moving to the most recent version of Shibboleth

G-Suite for Education

Shibboleth, with high interest in Azure SSO

AD and Azure AD, and Shibboleth

Shibboleth

Google SAML

Shibboleth IdP for library services, WS02 Identity for everything else.

ADFS and Shibboleth

What does your institution use for single sign-on (SSO)?

SecureAuth Identity Provider

Shibboleth

LDAP,ADFS,Azure,SAML

ADFS and Shibboleth

SAML 2.0 (via OneLogin)

We developed our own webauth in 2002 but we are moving to shibboleth.

ADFS

WSO2

Shibboleth

Shibboleth IdP v3

SAML/Shibboleth

Okta and Gluu

CAS

Active Directory

Okta

Shibboleth, CAS

Shibboleth

Shibboleth and CAS

Shibboleth SSO

Shibboleth

Okta

Shibbolth

Shibboleth IdP

Shibboleth and ADFS

What does your institution use for single sign-on (SSO)?

ADFS

IdentityNow and CAS

Okta

Shibboleth

OneLogin

Shibboleth IDP v 3.4.3

Shibboleth, custom applications

CAS and Shibboleth

ADFS

Fischer IdM

Shibboleth / CAS

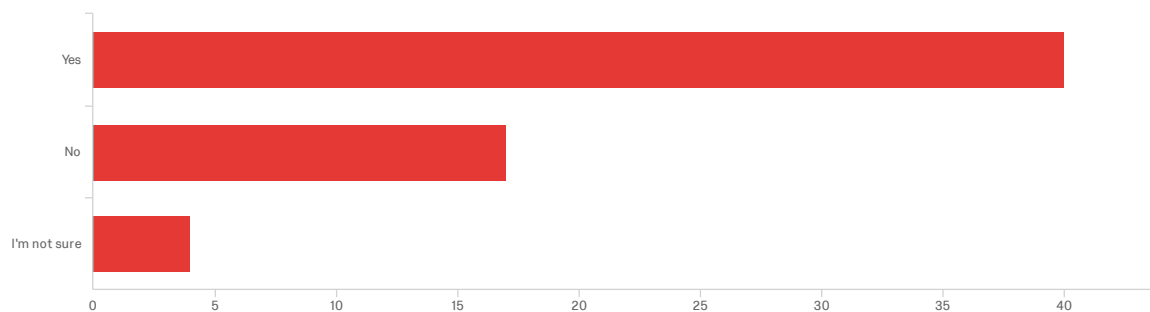
ADFS

shib, grouper, comanage

Shibboleth

Shibboleth

Q5 - Does your institution have an IdP registered with InCommon or in another federation that is a member of eduGAIN?

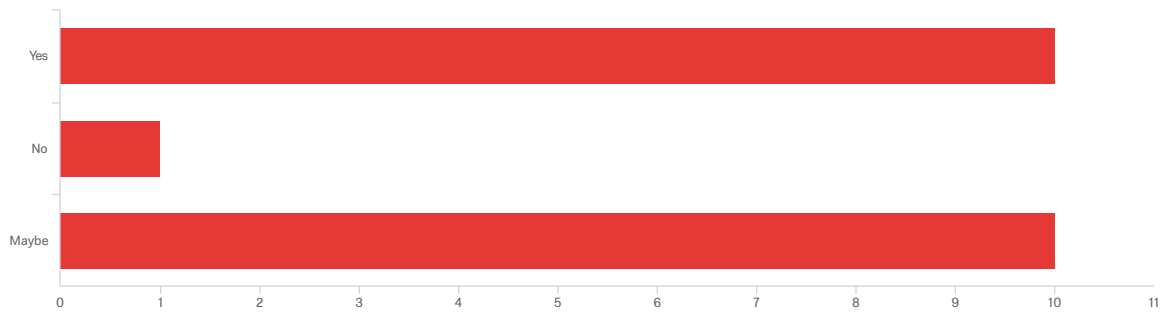


#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Does your institution have an IdP registered with InCommon or in another federation that is a member of eduGAIN?	1.00	3.00	1.41	0.61	0.37	61

#	Field	Choice Count
1	Yes	65.57% 40
2	No	27.87% 17
3	I'm not sure	6.56% 4
		61

Showing rows 1 - 4 of 4

Q6 - Is your institution interested in joining InCommon or another federation?



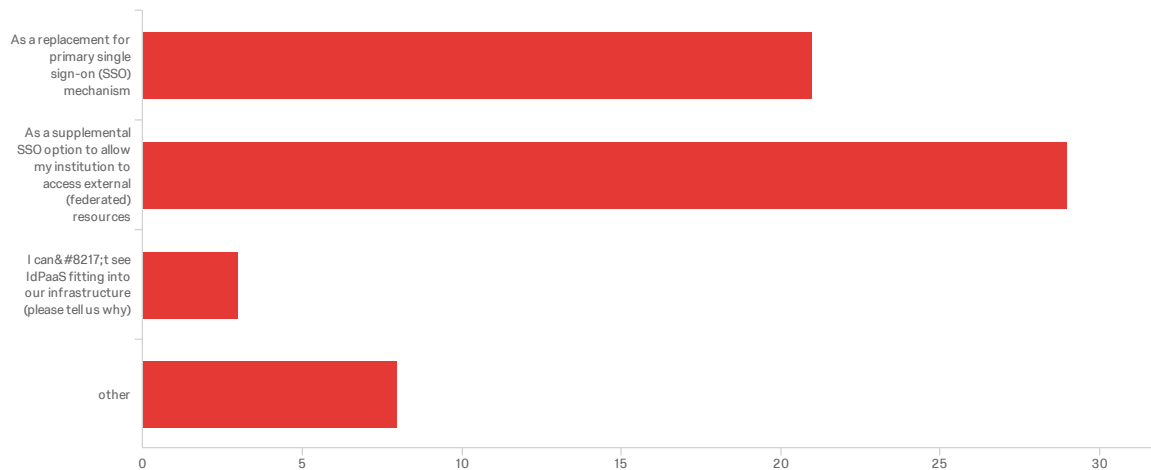
#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Is your institution interested in joining InCommon or another federation?	1.00	3.00	2.00	0.98	0.95	21

#	Field	Choice Count
1	Yes	47.62% 10
2	No	4.76% 1
3	Maybe	47.62% 10
		21

Showing rows 1 - 4 of 4

Q8 - IdPaaS INTEGRATION Where would you see IdPaaS as fitting into your institution's

IAM portfolio?



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	IdPaaS INTEGRATION Where would you see IdPaaS as fitting into your institution's IAM portfolio? - Selected Choice	1.00	4.00	1.97	0.96	0.92	61

#	Field	Choice Count
1	As a replacement for primary single sign-on (SSO) mechanism	34.43% 21
2	As a supplemental SSO option to allow my institution to access external (federated) resources	47.54% 29
3	I can't see IdPaaS fitting into our infrastructure (please tell us why)	4.92% 3
4	other	13.11% 8

61

Showing rows 1 - 5 of 5

Q8_3_TEXT - I can't see IdPaaS fitting into our infrastructure (please tell us why)

I can't see IdPaaS fitting into our infrastructure (please tell us why)

Prefer to keep authentication services on-prem

I can't see IdPaaS fitting into our infrastructure (please tell us why)

Currently, we already have our IDP hosted in AWS. We also use configuration management tools managing changes on our IDP.

Existing IDP meets our needs and can migrate to a cloud environment

Q8_4_TEXT - other

other

Supplement but perhaps eventually replace

It could easily be a little of the first two choices based on the configurability (as opposed to customizability) of the application. It can be assumed that it wouldn't be as customizable as a local instance but could give us the options we need to integrate with odd systems.

Not planning at this time. However, we are always considering this question in our future planning.

This could function as either a full replacement for our on-prem IdP or as a supplement.

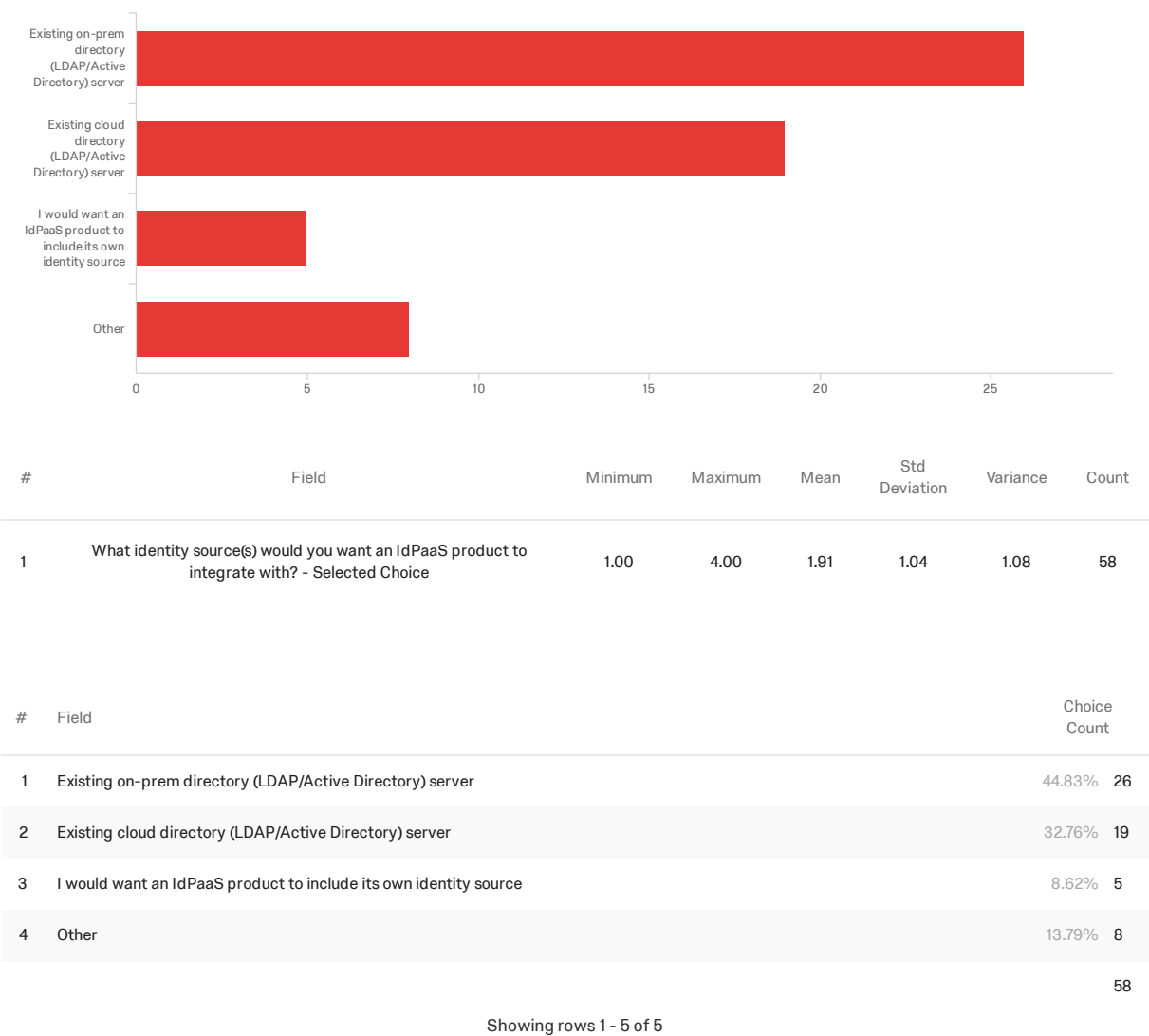
Potential means to reallocate staff to other services

Guest accounts

Not sure, need to understand overlap

For IAM, we'd likely want hybrid in some form

Q9 - What identity source(s) would you want an IdPaaS product to integrate with?



Q9_4_TEXT - Other

Other

Both on-prem and cloud once we get to a cloud directory;

Google SAML

I think this could be a mixture of all three depending on the applicationsn

On-prem

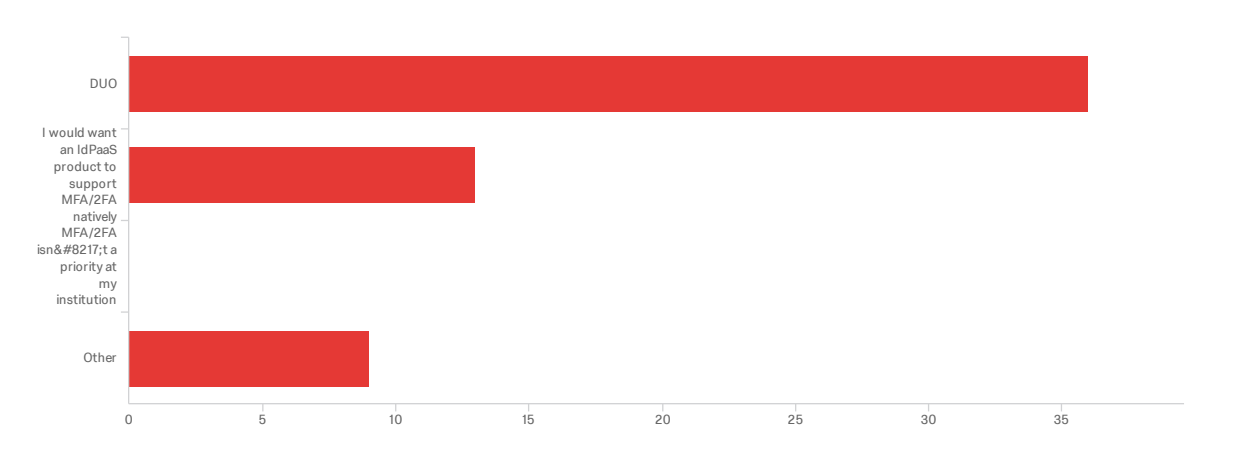
Other

Don't know what the right answer is here.

Existing shib IdP

LDAP/Kerberos (we do not put passwords in LDAP)

Q10 - What Multi-factor/Two-factor Authentication (MFA/2FA) services would you want to be supported?



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	What Multi-factor/Two-factor Authentication (MFA/2FA) services would you want to be supported? - Selected Choice	1.00	4.00	1.69	1.07	1.15	58

#	Field	Choice Count
1	DUO	62.07% 36
2	I would want an IdPaaS product to support MFA/2FA natively	22.41% 13
3	MFA/2FA isn't a priority at my institution	0.00% 0
4	Other	15.52% 9
		58

Showing rows 1 - 5 of 5

Q10_4_TEXT - Other

Other

Microsoft

Duo is the requirement; however, we also use Azure conditional access to support and drive Duo policies

Other

Any, really. It is important to have but I have very little preference. Google Authenticator is nice.

We currently use DUO and Azure MFA -- might want a hybrid approach

Both Duo and have support for generic MFA

Duo, Okta Verify, SMS, Voice

Right now we use DUO small scale but would be open to other options

Okta

Microsoft's MFA as well as DUO

Q11 - IdPaaS FEATURES How would the following features impact your interest in an IdPaaS solution?

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Supports consent and/or transparency about attribute release at time of login	1.00	5.00	2.03	0.85	0.72	58
2	Supports eduroam (includes RADIUSaaS)	1.00	5.00	1.81	1.09	1.19	58
3	Supports SAML Enhanced Client or Proxy (ECP) for non-browser-based authentication	1.00	5.00	1.98	1.03	1.05	58
4	Supports ability to integrate with vendors who are not part of InCommon or eduGAIN	1.00	4.00	1.43	0.65	0.42	58
5	Supports password reset	1.00	4.00	1.83	0.89	0.80	58
6	Supports institutional branding (colors, fonts, icons, etc.)	1.00	3.00	1.41	0.56	0.31	58
7	Supports site-specific attribute release policies (i.e., different sites can receive different levels of information about users)	1.00	3.00	1.41	0.62	0.38	58
8	Supports site-specific MFA/2FA policies (i.e., different sites can have different requirements)	1.00	5.00	1.67	0.86	0.74	58

#	Field	Must have		Desirable		Neutral		Not desirable		Not sure		Total
1	Supports consent and/or transparency about attribute release at time of login	27.59%	16	46.55%	27	22.41%	13	1.72%	1	1.72%	1	58
2	Supports eduroam (includes RADIUSaaS)	51.72%	30	29.31%	17	10.34%	6	3.45%	2	5.17%	3	58
3	Supports SAML Enhanced Client or Proxy (ECP) for non-browser-based authentication	36.21%	21	41.38%	24	15.52%	9	1.72%	1	5.17%	3	58
4	Supports ability to integrate with vendors who are not part of InCommon or eduGAIN	63.79%	37	31.03%	18	3.45%	2	1.72%	1	0.00%	0	58
5	Supports password reset	44.83%	26	32.76%	19	17.24%	10	5.17%	3	0.00%	0	58
6	Supports institutional branding (colors, fonts, icons, etc.)	62.07%	36	34.48%	20	3.45%	2	0.00%	0	0.00%	0	58
7	Supports site-specific attribute release policies (i.e., different sites can receive different levels of information about users)	65.52%	38	27.59%	16	6.90%	4	0.00%	0	0.00%	0	58
8	Supports site-specific MFA/2FA policies (i.e., different sites can have different requirements)	51.72%	30	34.48%	20	10.34%	6	1.72%	1	1.72%	1	58

Showing rows 1 - 8 of 8