1
00:00:00,080 --> 00:00:04,240
I'm Matthew Donkin
from AWS and I'm joined by Stephanie

2
00:00:04,240 --> 00:00:07,919
Lacey -- Stephanie do you want to come
on camera too?

3
00:00:07,919 --> 00:00:11,759
Sure that would be good as well
going to present some other lessons

4
00:00:11,759 --> 00:00:14,400
learned
for AWS from

5
00:00:14,400 --> 00:00:18,960
our first
OSCAL submission of an SSP to

6
00:00:18,960 --> 00:00:23,039
FedRAMP
and some of the things to be, kind of

7
00:00:23,039 --> 00:00:29,359
at a higher level. What we have
gone through to get it done and some of

8
00:00:29,359 --> 00:00:33,120
the lessons learned to share with others
and with that, I'm just

9
00:00:33,120 --> 00:00:35,920
going to dive right in

10
00:00:40,079 --> 00:00:43,200
so
The first thing is the format

11

00:00:43,200 --> 00:00:46,800
challenges. So one of the issues that
we've had was aligning some of our

12
00:00:46,800 --> 00:00:50,879
documentation and the various
documentation to the OSCAL format for

13
00:00:50,879 --> 00:00:55,199
specifically FedRAMP
with how our SSPs are written is

14
00:00:55,199 --> 00:00:59,520
very differently and we have various
dependencies which cause some issues

15
00:00:59,520 --> 00:01:02,800
Getting those into the proper format and
I'll go over that a little bit more on

16
00:01:02,800 --> 00:01:06,080
the next slide
And then, with our POA&M ... we have

17
00:01:06,080 --> 00:01:10,799
some extra information within our POA&M
as well that will be causing a little

18
00:01:10,799 --> 00:01:13,680
bit of issue in the future that we.. we're
kind of

19
00:01:13,680 --> 00:01:17,200
going to be working through it right now
But really, what it is right now, is taking

20
00:01:17,200 --> 00:01:19,920
that
that documentation and getting into that

21

00:01:19,920 --> 00:01:22,799
digitized format which we knew was not
going to be

22
00:01:22,799 --> 00:01:28,000
a very very easy lift. We knew there was
going to be issues setting out for this.

23
00:01:28,000 --> 00:01:31,840
So a lot of this was kind of like we
know what was going to happen and we are

24
00:01:31,840 --> 00:01:34,799
working through
various

25
00:01:34,799 --> 00:01:38,000
plans right now to
kind of get everything aligned for that

26
00:01:38,000 --> 00:01:41,840
machine relatable OSCAL format

27
00:01:42,000 --> 00:01:45,840
and the SSP challenges. So we have ... we
have our commercial boundary and our gov

28
00:01:45,840 --> 00:01:50,079
cloud boundary which each have a main
SSP and three appendices for each for the

29
00:01:50,079 --> 00:01:53,759
IaaS, PaaS and SaaS offerings and this
cause them

30
00:01:53,759 --> 00:01:58,320
trouble when we put it into the OSCAL
format for FedRAMP specifically. So

31
00:01:58,320 --> 00:02:03,920

we had to have a solution. Then our ...
temporary solution right now is just to

32
00:02:03,920 --> 00:02:08,640
have a separate OSCAL formatted SSP for
each of those

33
00:02:08,640 --> 00:02:13,520
 offerings. Right so you have one for IaaS PaaS and SaaS for our
commercial

34
00:02:13,520 --> 00:02:17,440
offerings and one for IaaS PaaS and SaaS
for our gov cloud offerings. As long as

35
00:02:17,440 --> 00:02:22,480
we got independence for all other appendices
for IL5. So it's seven documents

36
00:02:22,480 --> 00:02:26,560
right now for all of our SSPs and their
dependencies which is

37
00:02:26,560 --> 00:02:29,840
not
perfect but

38
00:02:29,840 --> 00:02:33,440
it's what we have for right now and
we're gonna be working towards that

39
00:02:33,440 --> 00:02:38,560
single two SSPs: right, one for commercial
one for gov cloud is what we want our end

40
00:02:38,560 --> 00:02:41,519
game to be in the future.

41
00:02:43,120 --> 00:02:46,319
And some of the implementation

challenges. There's multiple work streams

42
00:02:46,319 --> 00:02:50,000
that go
into providing this information and not

43
00:02:50,000 --> 00:02:55,840
all work streams were really on board at
first for OSCAL even um

44
00:02:55,840 --> 00:03:01,200
within our organization so we had to
really sell it and show the benefits

45
00:03:01,200 --> 00:03:03,840
right
and that is something that was actually

46
00:03:03,840 --> 00:03:08,480
fairly easy to do once you got into the
to what you could do with this

47
00:03:08,480 --> 00:03:13,200
particular format um and so once you get
people on board you get everybody moving

48
00:03:13,200 --> 00:03:17,360
in the same direction, it created issues
with managing that workflow. So instead

49
00:03:17,360 --> 00:03:23,519
of just managing for our one team we
have to now manage across multiple teams.

50
00:03:23,519 --> 00:03:26,879
And there's some erroneous information
that

51
00:03:26,879 --> 00:03:30,080
it was asked.

One of the .. one of the template

52
00:03:30,080 --> 00:03:33,200
issues was:
"How many users are on the cloud at one

53
00:03:33,200 --> 00:03:37,280
time". As you know
we're a very large

54
00:03:37,280 --> 00:03:40,640
hyperscaler cloud
company and ...

55
00:03:40,640 --> 00:03:44,239
to answer that question it's gonna be
different within 10 minutes. So

56
00:03:44,239 --> 00:03:47,360
and there's no N/A. You can't just say
this is not applicable to us so you have

57
00:03:47,360 --> 00:03:49,760
to put an answer in there and it's kind
of like well

58
00:03:49,760 --> 00:03:52,000
do you just put something in there and
this is going to be wrong in the next 10

59
00:03:52,000 --> 00:03:55,680
20 minutes or what what we do with that.
And then roles, of each individual

60
00:03:55,680 --> 00:03:59,280
working within the environment. We have
thousands of thousands of thousands of

61
00:03:59,280 --> 00:04:04,239
people working within the cloud at one

time. So providing that information

62
00:04:04,239 --> 00:04:08,159
and plus that changes too literally on a
daily basis, so providing that

63
00:04:08,159 --> 00:04:13,280
information for ... how they want it, is
kind of an implementation challenge

64
00:04:13,280 --> 00:04:16,640
that we are still working through.

65
00:04:17,040 --> 00:04:21,120
And with that, it had not been all
horrible!

66
00:04:21,120 --> 00:04:24,000
It hasn't been all just challenges. We have
some successes: we were the first

67
00:04:24,000 --> 00:04:29,520
obviously, with Telos, to provide the SSP
to FedRAMP, which is good because now we

68
00:04:29,520 --> 00:04:33,680
got the ball rolling on ironing out some
of the template issues, ironing out some

69
00:04:33,680 --> 00:04:37,759
of the schemas and and learning
ourselves what we need to do on our side

70
00:04:37,759 --> 00:04:41,040
to make this very successful and be able
to provide some of that feedback to

71
00:04:41,040 --> 00:04:44,639
industry partners and kind of continue
pushing the ball down the road.

72
00:04:44,639 --> 00:04:48,240
And we've ... also partnered with
Accenture 3PAO to pilot the first

73
00:04:48,240 --> 00:04:52,240
the pilot OSCAL authorization package
for some of our services. And we are going

74
00:04:52,240 --> 00:04:56,800
to provide the System Assessment Plan (SAP) and
System Assessment Report (SAR) to provide a

75
00:04:56,800 --> 00:05:00,800
complete OSCAL Authorization Package to
the FedRAMP JAB.

76
00:05:00,800 --> 00:05:05,600
And we hope to do that by Q4
of this year

77
00:05:06,000 --> 00:05:11,600
And some of the roadmap items right now:
-- We have the ... complete SSP again

78
00:05:11,600 --> 00:05:16,000
-- We're working on this SAP the SAR
and the POA&M -- We hope to have everything

79
00:05:16,000 --> 00:05:22,320
wrapped up by Q4 2022 to be able to
really be pushing this forward out in

80
00:05:22,320 --> 00:05:27,199
a usable way that can be ingested by our
customers

81
00:05:27,199 --> 00:05:32,000
And with that, I'm going to send it over
to Stephanie to discuss some of our ...

82
00:05:32,000 --> 00:05:36,320
some of XACTA's lessons learned as
well

83
00:05:36,960 --> 00:05:42,800
So telos has a solution that's called
XACTA and we help manage uh customers

84
00:05:42,800 --> 00:05:46,160
going through the RMF process and how
they can get accredited

85
00:05:46,160 --> 00:05:49,680
with FedRAMP.
But with

86
00:05:49,680 --> 00:05:52,680
OSCAL

87
00:05:58,240 --> 00:06:03,120
we had to address some challenges where
our models and our methods needed to be

88
00:06:03,120 --> 00:06:07,919
realigned to be able to export to an
OSCAL package.

89
00:06:07,919 --> 00:06:13,680
So we have a data exchange model, XDE,
but we needed to be able to translate

90
00:06:13,680 --> 00:06:18,479
the information within XDE into the
OSCAL structure.

91
00:06:18,479 --> 00:06:23,120
and also make sure that we identify... I
apologize for interrupting you. You are

92
00:06:23,120 --> 00:06:28,000
sharing the presenter's view. I don't
know if that is your

93
00:06:32,840 --> 00:06:39,360
intent. The swap displays button at the
top.. there! Yeah, there you go!

94
00:06:42,639 --> 00:06:47,840
So
we have a data machines model and it

95
00:06:47,840 --> 00:06:52,720
predates OSCAL, and then it was a way for
us to export and ingest information

96
00:06:52,720 --> 00:06:55,840
between
our XACTA solutions,

97
00:06:55,840 --> 00:07:00,080
but we needed to figure out how to get
our XDE

98
00:07:00,080 --> 00:07:06,479
into, or convert it into, an OSCAL format.
But then also make sure that we can

99
00:07:06,479 --> 00:07:10,720
support and balance future deployments
of our scale that don't necessarily

100
00:07:10,720 --> 00:07:15,280
follow the FedRAMP use case
and we also have to be able to ingest

101
00:07:15,280 --> 00:07:18,880
and process
these manual documents that are being

102
00:07:18,880 --> 00:07:22,639
provided to us,
put it into our tool so that we can

103
00:07:22,639 --> 00:07:26,800
format it and convert it into OSCAL

104
00:07:29,280 --> 00:07:32,560
so
one of the first things that we did was

105
00:07:32,560 --> 00:07:35,360
leverage both
our APIs

106
00:07:35,360 --> 00:07:40,160
our forum posts and various technologies
to ingest our

107
00:07:40,160 --> 00:07:45,280
handwritten SSPs,
manual POA&M, spreadsheets and data

108
00:07:45,280 --> 00:07:50,879
that's provided to the customer to get
it into XACTA, so that we can

109
00:07:50,879 --> 00:07:55,520
output the information.
What we also found was our

110
00:07:55,520 --> 00:08:00,800
original FedRAMP template while in line
with the original FedRAMP SSP, it needed

111
00:08:00,800 --> 00:08:06,160
some tweaks and modernization to be able
to output into the correct OSCAL format

112

00:08:06,160 --> 00:08:09,759
We were able to do some modernization of
our template

113
00:08:09,759 --> 00:08:15,360
to meet the OSCAL requirements
and then leverage

114
00:08:15,360 --> 00:08:22,479
the validation
schema to output our OSCAL SSP.

115
00:08:25,199 --> 00:08:27,840
And what we found was
we

116
00:08:27,840 --> 00:08:32,640
want to be able to add new API endpoints
and new calls

117
00:08:32,640 --> 00:08:36,479
to
be able to not just output but ingest

118
00:08:36,479 --> 00:08:41,360
some additional OSCAL information
especially as the model matures more and

119
00:08:41,360 --> 00:08:45,519
there are additional catalog pieces and
customer information that we need to be

120
00:08:45,519 --> 00:08:49,120
able to pull into
XACTA.

121
00:08:49,120 --> 00:08:53,440
We've also worked with NIST and FedRAMP
to create a feedback loop process just

122

00:08:53,440 --> 00:08:58,080
to address unique challenges or use
cases that fall within these areas to

123
00:08:58,080 --> 00:09:02,560
make sure we're still meeting the core
requirements of NIST OSCAL

124
00:09:02,560 --> 00:09:07,040
while addressing the unique use cases of
FedRAMP

125
00:09:07,040 --> 00:09:12,320
And leveraging the catalogs provided
by this to make sure that we are

126
00:09:12,320 --> 00:09:16,640
matching the information up with the
core base model

127
00:09:16,640 --> 00:09:21,360
so our future OSCAL deliverables and
development are underway. So we're

128
00:09:21,360 --> 00:09:26,080
working now towards outputting the POA&M
model.

129
00:09:26,080 --> 00:09:31,279
We're also exploring catalog and profile
generation for our regulations that we

130
00:09:31,279 --> 00:09:37,839
have inside XACTA that are not
800-53 based

131
00:09:37,839 --> 00:09:42,959
That way we can support customers who
need to meet other regulations

132

00:09:42,959 --> 00:09:45,839
and want to be able to use the OSCAL
models

133
00:09:45,839 --> 00:09:50,240
and we're also right now conducting
analysis for SAP and SAR models to make

134
00:09:50,240 --> 00:09:55,720
sure we can output the full OSCAL
package.

135
00:10:04,399 --> 00:10:07,760
I think that's everything

136
00:10:08,240 --> 00:10:13,120
That's fantastic thank you. Thank you so
much. So if this is the

137
00:10:13,120 --> 00:10:18,480
end of the presentation, with your
permission, I'm going to stop the recording.