1
00:00:01,199 --> 00:00:06,000
everybody in this OSCAL community good

2
00:00:04,240 --> 00:00:07,359
morning good afternoon good evening

3
00:00:06,000 --> 00:00:09,519
whenever you

4
00:00:07,359 --> 00:00:13,040
will listen to the recording

5
00:00:09,519 --> 00:00:14,920
the topic of today is an open source

6
00:00:13,040 --> 00:00:16,640
um

7
00:00:14,920 --> 00:00:19,119
implementation

8
00:00:16,640 --> 00:00:21,600
of oscar

9
00:00:19,119 --> 00:00:23,920
uh the tool is called trestle

10
00:00:21,600 --> 00:00:27,199
and uh we are going through the

11
00:00:23,920 --> 00:00:29,840
details and uh a demo uh so myself and

12
00:00:27,199 --> 00:00:31,119
gikas will will present and will help us

13
00:00:29,840 --> 00:00:34,640

with the demo

14
00:00:31,119 --> 00:00:37,200
so before we start i would like to um

15
00:00:34,640 --> 00:00:39,760
before we get into the threshold details

16
00:00:37,200 --> 00:00:40,640
two slides on uh

17
00:00:39,760 --> 00:00:43,440
our

18
00:00:40,640 --> 00:00:46,960
vision in terms of uh compliance

19
00:00:43,440 --> 00:00:49,280
personas roles and their leverage of the

20
00:00:46,960 --> 00:00:51,520
oscar artifacts

21
00:00:49,280 --> 00:00:54,000
uh i i know that different terminologies

22
00:00:51,520 --> 00:00:56,079
are used in in different contexts i just

23
00:00:54,000 --> 00:00:58,559
wanted here to just give our

24
00:00:56,079 --> 00:01:01,280
interpretation of of the trends so that

25
00:00:58,559 --> 00:01:03,039
you do not start discussions on on

26
00:01:01,280 --> 00:01:04,879
terminology and just to understand what

27
00:01:03,039 --> 00:01:07,439
we mean and and we can

28
00:01:04,879 --> 00:01:08,640
uh change terms or you know in uh

29
00:01:07,439 --> 00:01:10,320
offline

30
00:01:08,640 --> 00:01:12,240
so for a

31
00:01:10,320 --> 00:01:14,240
typical government risk and compliance

32
00:01:12,240 --> 00:01:18,080
framework right from the compliance

33
00:01:14,240 --> 00:01:21,439
perspective point of view uh we um are

34
00:01:18,080 --> 00:01:22,720
uh looking with trestle to support the

35
00:01:21,439 --> 00:01:27,040
regulators

36
00:01:22,720 --> 00:01:29,759
uh with their you know definition of um

37
00:01:27,040 --> 00:01:31,439
and as issuers of catalogs and

38
00:01:29,759 --> 00:01:34,799

predefined profiles

39
00:01:31,439 --> 00:01:37,200
we are supporting control providers um

40
00:01:34,799 --> 00:01:38,840
we are looking like system

41
00:01:37,200 --> 00:01:42,880
software

42
00:01:38,840 --> 00:01:45,040
hardware service vendors uh to

43
00:01:42,880 --> 00:01:47,920
support to declare their product

44
00:01:45,040 --> 00:01:50,399
compliance implementation as uh

45
00:01:47,920 --> 00:01:52,799
technical rules with the parameters and

46
00:01:50,399 --> 00:01:55,840
mappings to the catalogs

47
00:01:52,799 --> 00:01:57,600
the control providers can also take as

48
00:01:55,840 --> 00:01:59,360
input um

49
00:01:57,600 --> 00:02:00,399
additional guidance from profiles

50
00:01:59,360 --> 00:02:02,000
provided

51
00:02:00,399 --> 00:02:04,960
from cso

52
00:02:02,000 --> 00:02:07,439
um cso define profiles

53
00:02:04,960 --> 00:02:09,440
uh and assign them to the environments

54
00:02:07,439 --> 00:02:12,080
that are subscribed to by the system

55
00:02:09,440 --> 00:02:13,280
owners the system owners are responsible

56
00:02:12,080 --> 00:02:16,560
to ensure

57
00:02:13,280 --> 00:02:18,879
that their systems are compliant and

58
00:02:16,560 --> 00:02:20,840
they work with assessment results and

59
00:02:18,879 --> 00:02:23,680
may recommend

60
00:02:20,840 --> 00:02:27,280
remediations um

61
00:02:23,680 --> 00:02:29,120
we are indirectly uh supporting operator

62
00:02:27,280 --> 00:02:30,959
administration and devops

63
00:02:29,120 --> 00:02:34,800

uh in the sense that

64
00:02:30,959 --> 00:02:34,800
we understand that they need to

65
00:02:35,040 --> 00:02:41,599
consume um assessment results and um

66
00:02:39,519 --> 00:02:45,280
uh plans of actions

67
00:02:41,599 --> 00:02:46,480
and the uh goal of trestle is to really

68
00:02:45,280 --> 00:02:47,519
generate

69
00:02:46,480 --> 00:02:50,640
um

70
00:02:47,519 --> 00:02:51,680
as much as possible automatically

71
00:02:50,640 --> 00:02:54,800
the

72
00:02:51,680 --> 00:02:58,800
system security plan for the auditors

73
00:02:54,800 --> 00:02:59,599
and uh structure the assessment results

74
00:02:58,800 --> 00:03:04,319
for

75
00:02:59,599 --> 00:03:05,360
benefits of reports and supports um the

76
00:03:04,319 --> 00:03:07,440
um

77
00:03:05,360 --> 00:03:09,760
as an sdk we will see the development of

78
00:03:07,440 --> 00:03:12,800
any type of translation so those

79
00:03:09,760 --> 00:03:14,159
artifacts can be translated any template

80
00:03:12,800 --> 00:03:14,380
that uh

81
00:03:14,159 --> 00:03:15,680
the

82
00:03:14,380 --> 00:03:18,640
[Music]

83
00:03:15,680 --> 00:03:22,159
third party auditors will make available

84
00:03:18,640 --> 00:03:23,840
we also have the control uh assessors so

85
00:03:22,159 --> 00:03:26,799
in in

86
00:03:23,840 --> 00:03:30,560
this the context of this presentation

87
00:03:26,799 --> 00:03:32,560
the control assessors are those that

88
00:03:30,560 --> 00:03:34,799

develop products

89
00:03:32,560 --> 00:03:37,680
that uh

90
00:03:34,799 --> 00:03:39,200
post the checks that will test the rules

91
00:03:37,680 --> 00:03:41,360
the technical rules that the control

92
00:03:39,200 --> 00:03:42,799
providers declared

93
00:03:41,360 --> 00:03:44,000
as being

94
00:03:42,799 --> 00:03:45,200
the way that the controls are

95
00:03:44,000 --> 00:03:46,799
implemented

96
00:03:45,200 --> 00:03:48,879
and

97
00:03:46,799 --> 00:03:50,560
and that can be from uh for an actual

98
00:03:48,879 --> 00:03:52,799
environment or for a reference

99
00:03:50,560 --> 00:03:55,360
architecture if we have the

100
00:03:52,799 --> 00:03:57,360
uh cicd artifacts like terraform

101
00:03:55,360 --> 00:04:00,720
infrastructures code files

102
00:03:57,360 --> 00:04:04,080
um and the control assessors are um

103
00:04:00,720 --> 00:04:06,799
expected to consume a profile or an ssp

104
00:04:04,080 --> 00:04:09,599
and uh provide posture results so now

105
00:04:06,799 --> 00:04:11,360
let's see how in in trestle we map these

106
00:04:09,599 --> 00:04:13,200
two um

107
00:04:11,360 --> 00:04:16,000
to the oscar

108
00:04:13,200 --> 00:04:18,560
artifacts so the regulators as control

109
00:04:16,000 --> 00:04:20,479
issuers will manage a catalog we see at

110
00:04:18,560 --> 00:04:22,800
the bottom of the page right those

111
00:04:20,479 --> 00:04:26,639
catalogs contain controls here is an

112
00:04:22,800 --> 00:04:28,560
example of list 853 sc 74

113
00:04:26,639 --> 00:04:31,360

um we

114
00:04:28,560 --> 00:04:33,199
expect the compliance officers or csos

115
00:04:31,360 --> 00:04:35,440
to

116
00:04:33,199 --> 00:04:37,040
use the profiles

117
00:04:35,440 --> 00:04:40,160
to

118
00:04:37,040 --> 00:04:41,680
provide a subset of a catalog

119
00:04:40,160 --> 00:04:44,560
or to add

120
00:04:41,680 --> 00:04:47,280
additional guidance as an interpretation

121
00:04:44,560 --> 00:04:50,400
of a particular control with that um

122
00:04:47,280 --> 00:04:52,639
corporate or that uh that

123
00:04:50,400 --> 00:04:54,240
particular group

124
00:04:52,639 --> 00:04:56,240
and of course the profile being a

125
00:04:54,240 --> 00:05:01,360
transformation on the catalog it don't

126
00:04:56,240 --> 00:05:02,960
contain uh the the controls of the um

127
00:05:01,360 --> 00:05:04,240
catalogs that have been referred in that

128
00:05:02,960 --> 00:05:06,720
profile

129
00:05:04,240 --> 00:05:08,960
then we move to the uh control and so we

130
00:05:06,720 --> 00:05:11,520
can consider the compliance officers and

131
00:05:08,960 --> 00:05:14,400
ciso as being the control owners

132
00:05:11,520 --> 00:05:16,160
so um we move to control providers this

133
00:05:14,400 --> 00:05:20,320
being the software hardware service

134
00:05:16,160 --> 00:05:20,320
providers and um we

135
00:05:21,120 --> 00:05:25,039
provide the component definition right

136
00:05:22,960 --> 00:05:27,680
we implement the support of oscar

137
00:05:25,039 --> 00:05:29,440
component definition for them to declare

138
00:05:27,680 --> 00:05:31,680

uh the

139
00:05:29,440 --> 00:05:34,960
the implementation of the controls and

140
00:05:31,680 --> 00:05:36,880
we will see how we uh repurposed the

141
00:05:34,960 --> 00:05:39,360
properties right of the control in order

142
00:05:36,880 --> 00:05:41,199
to define the rules that the technical

143
00:05:39,360 --> 00:05:43,840
controls that that actually can be

144
00:05:41,199 --> 00:05:46,400
actually measured um and the checks that

145
00:05:43,840 --> 00:05:48,080
are associated with that to validate

146
00:05:46,400 --> 00:05:49,360
that that particular

147
00:05:48,080 --> 00:05:51,680
technical check and you see some

148
00:05:49,360 --> 00:05:54,560
examples there for

149
00:05:51,680 --> 00:05:58,080
implementation in kubernetes or in flow

150
00:05:54,560 --> 00:06:00,400
logs of sc74 so

151
00:05:58,080 --> 00:06:02,880
these are these are technical controls

152
00:06:00,400 --> 00:06:07,120
in kubernetes and in flow log that have

153
00:06:02,880 --> 00:06:08,319
uh implement an aspect of sc74

154
00:06:07,120 --> 00:06:11,680
as i mentioned in the component

155
00:06:08,319 --> 00:06:14,400
definition we also map uh the um

156
00:06:11,680 --> 00:06:17,120
technical rules uh to the

157
00:06:14,400 --> 00:06:20,720
uh checks right to the the the

158
00:06:17,120 --> 00:06:23,120
the code that tests the the rules

159
00:06:20,720 --> 00:06:26,160
we will see that those checks uh

160
00:06:23,120 --> 00:06:27,919
can be um declarative or can be

161
00:06:26,160 --> 00:06:29,360
imperative depending on the language

162
00:06:27,919 --> 00:06:33,600
that is used

163
00:06:29,360 --> 00:06:36,560

so well they are not part of trestle uh

164
00:06:33,600 --> 00:06:39,120
this we we move into the from the realm

165
00:06:36,560 --> 00:06:42,000
of oscar compliances code into the realm

166
00:06:39,120 --> 00:06:44,000
of policy as code so that's why this is

167
00:06:42,000 --> 00:06:45,759
gray out here right we expect that is

168
00:06:44,000 --> 00:06:47,919
you know a different repository uh

169
00:06:45,759 --> 00:06:52,000
different type of skills that are are

170
00:06:47,919 --> 00:06:55,280
required to to develop those uh

171
00:06:52,000 --> 00:06:56,400
to develop those checks and um

172
00:06:55,280 --> 00:06:58,000
the

173
00:06:56,400 --> 00:07:01,520
the

174
00:06:58,000 --> 00:07:03,440
what is relevant and and uh critical at

175
00:07:01,520 --> 00:07:06,000
the oscar level at the compliances code

176
00:07:03,440 --> 00:07:08,639
is the mapping from the the technical

177
00:07:06,000 --> 00:07:11,440
checks to those rules because the

178
00:07:08,639 --> 00:07:13,599
results provided by those checks

179
00:07:11,440 --> 00:07:16,000
um uh will

180
00:07:13,599 --> 00:07:17,440
be the basis

181
00:07:16,000 --> 00:07:20,479
of the

182
00:07:17,440 --> 00:07:21,840
observations that are aggregated through

183
00:07:20,479 --> 00:07:23,919
the

184
00:07:21,840 --> 00:07:25,759
mapping that is uh provided by the

185
00:07:23,919 --> 00:07:28,800
vendor in component definition will be

186
00:07:25,759 --> 00:07:32,080
aggregated up into the control finding

187
00:07:28,800 --> 00:07:34,319
so that we are able to uh provide the uh

188
00:07:32,080 --> 00:07:36,880

posture right from the regulation point

189
00:07:34,319 --> 00:07:37,680
of view rather than from the um

190
00:07:36,880 --> 00:07:39,919
the

191
00:07:37,680 --> 00:07:42,400
product rules point of view and of

192
00:07:39,919 --> 00:07:45,520
course in case of failures will uh

193
00:07:42,400 --> 00:07:47,759
support the association with tasks in

194
00:07:45,520 --> 00:07:49,360
the plan of actions that those can be

195
00:07:47,759 --> 00:07:52,800
remediations

196
00:07:49,360 --> 00:07:54,160
um because in this case ibm is a uh in

197
00:07:52,800 --> 00:07:55,919
our case we

198
00:07:54,160 --> 00:07:58,479
are a cloud provider most of the

199
00:07:55,919 --> 00:07:59,759
remediations are

200
00:07:58,479 --> 00:08:00,800
most of the

201
00:07:59,759 --> 00:08:04,479
the

202
00:08:00,800 --> 00:08:06,160
tasks are remediations uh but of course

203
00:08:04,479 --> 00:08:07,599
we uh

204
00:08:06,160 --> 00:08:10,400
we are aware that

205
00:08:07,599 --> 00:08:12,720
those can be other type of uh

206
00:08:10,400 --> 00:08:14,560
actions like um

207
00:08:12,720 --> 00:08:17,599
um

208
00:08:14,560 --> 00:08:18,639
exceptions from the from the profile and

209
00:08:17,599 --> 00:08:21,919
so on

210
00:08:18,639 --> 00:08:23,759
so with with that um

211
00:08:21,919 --> 00:08:25,120
uh if there are no uh and we take

212
00:08:23,759 --> 00:08:27,120
questions at the end okay so with that

213
00:08:25,120 --> 00:08:29,599

we will i'll hand the

214
00:08:27,120 --> 00:08:31,520
mic to vcus and

215
00:08:29,599 --> 00:08:35,399
we will go into the details of how

216
00:08:31,520 --> 00:08:35,399
tressel is implementing