



C2 LABS
TAKE BACK CONTROL

Cyber Security Controls: Data Portability between vendor tools using NIST OSCAL

J. Travis Howerton
Chief Technology Officer (CTO)
C2 Labs

<https://www.c2labs.com>

<https://atlasity.io>



WHO WE ARE



C2 LABS
TAKE BACK CONTROL

Who We Are

About Us

- **Minority-Owned DC small business:** Founded in 2014, with a diverse workforce & strong nationwide commercial and government past performance
- **Mission:** To serve as a security focused and agile digital transformation partner that blends *Art* and *Science* to enable our customers to expand their vision, drive cultural change, and avoid being left behind
- **Certifications and Awards:** PMP, ITIL, CISSP, DAWIA, AWS, Agile SCRUM Masters, Fed100 Award, ACT-IAC Excellence.gov overall award winner (Most innovative project in Government)

Key Cultural Values

- I nnovative
- D riven
- E thical
- A gile
- S ervice

“Logic will get you from A to B.
 Imagination will take you everywhere”
 – Albert Einstein



Bio – J. Travis Howerton, C2 Labs Chief Technology Officer



- Travis Howerton is the co-founder and Chief Technology Officer (CTO) of C2 Labs and has previously held positions as the National Nuclear Security Administration CTO, Deputy CIO at Oak Ridge National Laboratory, and the Global Director for Strategic Programs with Bechtel Corporation.
- Howerton holds a B.S. in Organizational Management from Tusculum College, a M.S. in Computer Information Systems from Boston University, and holds multiple certifications to include the CISSP, ITIL, PMP, Scrum Master, Harvard Credential of Readiness, and AWS Certified Developer.
- Howerton is a native of Oak Ridge, TN where he lives with his wife (Beth) and two daughters (Taylor and Sarah Beth).

Abstract

Today, System Security Plans (SSPs) are usually generated in Word or Excel documents using unstructured formats that make them difficult to process in an automated way or to port the information across tools due to the wide variability in formats. In this session, we will discuss how NIST's OSCAL standard can enable cyber security control data portability, moving cyber security risk and assessment information across different vendor tools using the OSCAL format. By leveraging OSCAL, we will demonstrate:

- The ability to load all OSCAL Catalogs and Baselines of NIST SP 800-53 Rev 4, 5, and FedRAMP Baselines (Low, Moderate, High, and Privacy) into the C2 Labs Atlasity tool
- The ability to load an OSCAL version of an SSP from GovReady (another vendor tool) into Atlasity
- The ability to cross-walk controls from the GovReady SSP against the NIST SP 800-53 FedRAMP Moderate Baseline to load programmatically into Atlasity
- The ability to support leveraged authorizations within Atlasity in support of the OSCAL standard

Hypotheses

This proposal sought to test two hypotheses of the effectiveness of using OSCAL to programmatically load content. These include:

- OSCAL can be used to efficiently load NIST controls to allow the rapid creation of security plans
 - EXAMPLE BENEFIT: Improved quality and time to value by automating the creation of SSPs
- OSCAL can be used to efficiently transfer SSP content programmatically between tools
 - EXAMPLE BENEFIT: Cloud Service Providers could submit SSP content in an automated manner to perform compliance checks with less manual labor and resulting costs (i.e. to FedRAMP)

Experiment 1 – Loading Catalogs and Creating a SSP

Python Script for Loading (271 lines of code)

```
master atlasify / oscal / importer.py <> Jump to - Go to file ...
howieavp76 Importer Fix Latest commit 80390ec on Nov 15 History
1 contributor
275 lines (239 sloc) | 10.7 KB Raw Blame
1 #!/usr/bin/python
2 # This code sample uses the 'requests' library:
3 # http://docs.python-requests.org
4 import requests
5 from requests.auth import HTTPBasicAuth
6 import json
7 import argparse
8
9 # setup parser for command line arguments
10 parser = argparse.ArgumentParser(description='Atlasify parser for NIST 800-53 OSCAL')
11 parser.add_argument('token', metavar='path', type=str, help='Atlasify JMT token to authenticate API calls')
12
13 # get the argument from the command line
14 args = parser.parse_args()
15 if (args.token == ''):
16     print('No JWT Bearer token provided.')
17 else:
18     print(args.token)
19     token = args.token
20
21 # set the catalog URL for your Atlasify instance
22 url_cats = "http://localhost:5000/api/catalogues"
23
24 # set your bearer token (Click your name in top right and select Service Accounts, paste Bearer token from this page)
25 headers = {
26     'Authorization': 'Bearer ' + token
27 }
28
29 # setup catalog data
30 cat = {
31     "title": "NIST 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations",
32     "description": "This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets",
33     "datePublished": "9/1/2020",
34     "lastRevisionDate": "9/1/2020",
35     "url": "https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final",
36     "abstract": "This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets",
37     "keywords": "assurance; availability; computer security; confidentiality; control; cybersecurity; FISMA; information security; information system; integrity; personally id",
38     "createdById": "8d8d5468-74f8-499d-976c-bca671e19b14",
39     "lastUpdatedById": "8d8d5468-74f8-499d-976c-bca671e19b14" }
40
```

- C2 Labs downloaded the latest NIST 800-53 and FedRAMP Baselines from the [OSCAL GitHub site](https://github.com/C2-Labs/atlasify)
- Developed an open-source Python script to parse the OSCAL baseline JSON files, enriched with other data, and bulk uploaded them as catalogs via [REST APIs](#) in [Atlasify](#) (also published interim artifacts in JSON)
- Developed many Atlasify profiles based on NIST 800-53 Rev. 4, Rev. 5, and FedRAMP
- Used our SSP wizard to create a security plan template in less than 5 minutes after import
- Source code open-sourced [@Atlasify](#)

EVIDENCE ON GITHUB:

<https://github.com/C2-Labs/atlasify/tree/master/oscal>

Level of Effort: ~ 15 hours

README: contains detailed process and results info



Experiment 1 – Results

SUCCESS

Catalogs Loaded

Actions	ID #	Title	Date Published	URL
View	94	DSS Electronic Communications Plan	09/01/2011	https://www.dcsa.mil/mc/ctp/foci/
View	91	NIST 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations - PRIVACY Baseline	09/23/2020	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
View	90	NIST 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations - LOW Baseline	09/23/2020	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
View	89	NIST 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations - MODERATE Baseline	09/23/2020	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
View	88	NIST 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations - HIGH Baseline	09/23/2020	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
View	87	NIST 800-53 Rev. 4 - Security and Privacy Controls for Information Systems and Organizations - Tailored Low Impact Software as a Service (LI-SaaS) Baseline	01/22/2015	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
View	86	NIST 800-53 Rev. 4 - Security and Privacy Controls for Information Systems and Organizations - FedRAMP LOW Baseline	01/22/2015	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
View	85	NIST 800-53 Rev. 4 - Security and Privacy Controls for Information Systems and Organizations - FedRAMP MODERATE Baseline	01/22/2015	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
View	84	NIST 800-53 Rev. 4 - Security and Privacy Controls for Information Systems and Organizations - FedRAMP HIGH Baseline	01/22/2015	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
View	82	NIST 800-53 Rev. 4 - Security and Privacy Controls for Information Systems and Organizations - LOW Baseline	01/22/2015	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
View	81	NIST 800-53 Rev. 4 - Security and Privacy Controls for Information Systems and Organizations - MODERATE Baseline	01/22/2015	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

Profiles Created

SECURITY PROFILE FORM

ID # 38

Security Profile Name *
800-53 Rev 5 Moderate

Profile Owner *
Howerton, Travis (howieavp)

RIF5 Categorization *
Moderate

Custom Fields

Is low profile *
No

Toolbar
[Save](#) [Delete](#) [Back](#) [View](#) [Create New](#) [Jump to Top](#)

Subsystems
[Compliance Explorer](#) [Workflows](#) [Social](#) [Files](#) [Links](#) [Stakeholders](#) [History](#) [Time Travel](#) [Timeline](#) [Profile Mapping](#)

SHOW SELECTED CONTROLS
[Map Controls to Profile](#)

SELECTED CONTROLS 323

Action	Control Name	Description
View	AC1 - Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access control; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Discussion



Experiment 1 – Results

SUCCESS

SSP Creation

The screenshot shows the 'SECURITY PLAN FORM' in the ATLASITY application. The form is titled 'ID # 66' and has a 'Jump to Toolbar' button. It is divided into several sections: 'Basic Information', 'Categorization', 'Key Dates', 'Description', 'Stakeholders and Users', and 'Custom Fields'. The 'Categorization' section shows 'Moderate' and 'Status: Under Development'. The 'System Name' is 'NIST OSCAL Workshop 2021'. The 'Other Identifier' is empty. The 'Status' is 'Under Development'. The 'System Type' is 'General Support System'. The 'Facility' is 'C2 Labs HQ'. The 'Toolbar' contains buttons for 'Save', 'Delete', 'Back', 'Print', 'Email', 'Export', 'Create New', and 'Jump to Top'. Below the form is the 'Security Plan Visualizer' section, which includes a 'Security Plan Builder' button and four steps: 'Step 1 - Instructions', 'Step 2 - Profile', 'Step 3 - Manual', and 'Step 4 - Finish'. A welcome message reads: 'Welcome to the Security Plan Builder! This wizard provides an easy way to create standardized security plans from templates known as security profiles. The steps to create a security plan are as follows: Select the applicable security profile from the profile list. This step will automatically add all of the controls from the profile to the security plan. Manually add any additional controls that may apply. Confirm that the selected controls are correct and click "Finish" to build your security plan.'

SSP Visualization

The screenshot shows the 'Security Plan Visualizer' in the ATLASITY application. The system name is 'NIST OSCAL Workshop 2021'. The 'Other Identifier' is empty. The 'Status' is 'Under Development'. The 'System Type' is 'General Support System'. The 'Facility' is 'C2 Labs HQ'. The 'Toolbar' contains buttons for 'Save', 'Delete', 'Back', 'Print', 'Email', 'Export', 'Create New', and 'Jump to Top'. The 'Security Plan Visualizer' section includes a 'Security Plan Builder' button and four charts: 'CONTROLS BY STATUS', 'CONTROLS BY LAST ASSESSMENT RESULT', 'CONTROLS BY OWNER', and 'CONTROLS BY DATE LAST ASSESSED'. The 'CONTROLS BY STATUS' chart shows a donut chart with a red segment for 'Not Implemented'. The 'CONTROLS BY LAST ASSESSMENT RESULT' chart shows a donut chart with a red segment. The 'CONTROLS BY OWNER' chart shows a donut chart with a red segment for 'Howerton, Travis'. The 'CONTROLS BY DATE LAST ASSESSED' chart shows a bar chart with a y-axis from 0 to 324.0 and an x-axis with a value of 5.1. Below the charts is the 'Subsystems' section, which includes a 'Compliance Explorer' button and a list of subsystems: 'Workflows', 'Social', 'Files', 'Links', 'Stakeholders', 'History', 'Time Travel', and 'Timeline'. The 'Security Plan: NIST OSCAL Workshop 2021' section includes an 'Add Child Record' button and a 'Control Implementations' button with a '323' indicator.



Experiment 2 – Loading OSCAL SSP from GovReady

Python Script for Loading (662 lines of code)

```
master atlasify / oscal-ssp-import / importer.py / <> Jump to - Go to file ...
howieavp76 Controls Uploaded Latest commit e9cb287 21 hours ago History
1 contributor
662 lines (624 sloc) 25.3 KB Raw Blame
1 #!/usr/bin/python
2 # This code sample uses the 'requests' library:
3 # http://docs.python-requests.org
4 import requests
5 from requests.auth import HTTPBasicAuth
6 import json
7 import argparse
8
9 class Logger:
10     OK = '\033[92m'
11     WARNING = '\033[93m'
12     ERROR = '\033[91m'
13     END = '\033[0m'
14
15 # setup parser for command line arguments
16 parser = argparse.ArgumentParser(description='Atlasify parser for NIST 800-53 OSCAL')
17 parser.add_argument('--user', metavar='path', type=str, help='Atlasify username')
18 parser.add_argument('--pwd', metavar='path', type=str, help='Atlasify password')
19 parser.add_argument('--catalog', metavar='path', type=str, help='Atlasify catalog containing security controls for this SSP')
20
21 # get the argument from the command line
22 args = parser.parse_args()
23 if (args.user == ''):
24     print('ERROR: No username provided.')
25     exit
26 else:
27     strUser = args.user
28 if (args.pwd == ''):
29     print('ERROR: No password provided.')
30     exit
31 else:
32     strPWD = args.pwd
33 if (args.pwd == ''):
34     print('ERROR: No password provided.')
35     exit
36 else:
37     intCatalog = args.catalog
38
39 # set the catalog URL for your Atlasify instance
40 url_login = "http://localhost:5000/api/authentication/login"
41
```

- The [GovReady](#) team provided an example SSP from their tool in OSCAL format for C2 Labs to process
- Developed an open-source Python script to parse the OSCAL SSP JSON file to create the SSP and Control Implementations in [Atlasify](#)
- Mapped schema differences between GovReady and Atlasify with OSCAL
- Loaded data programmatically via [Atlasify REST APIs](#)
- Source code open-sourced [@Atlasify](#)

EVIDENCE ON GITHUB:

<https://github.com/C2-Labs/atlasify/tree/master/oscal-ssp-import>

Level of Effort: ~ 30 hours

README: contains detailed process and results info



Experiment 2 – Results

SSP Loading (Raw Logs)

```
oscal-sip-import > importer.py ...
1 #!/usr/bin/python
2 # This code sample uses the 'requests' library:
3 # http://docs.python-requests.org
4 import requests
5 from requests.auth import HTTPBasicAuth
6 import json
7 import argparse
8
9 class Logger:
10     OK = "\033[0m"
11     WARNING = "\033[033m"
12     ERROR = "\033[31m"
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
263
```

Experiment 2 – Results MVP 1



SSP Details

ATLASITY Home Status Boards My Workbench News Feed Modules Calendar

Integrity: Moderate

Availability: Moderate

Overall Categorization: Moderate

High Value Asset (HVA): false

Description:
System Metadata
Version: 0.0
Imported Using OSCAL Version: 1.0-Milestone3
Remarks: This OSCAL-based FedRAMP SSP Template can be used for the FedRAMP Low, Moderate, and High baselines. In Guidance for OSCAL-based FedRAMP Tailored content has not yet been developed.

System Properties
marking: Controlled Unclassified Information

Revision History
Version: 1.0, Date Published: 2019-06-01T00:00:00-04:00, OSCAL Version: 1.0-Milestone3, Remarks: Initial publication.
Version: 2.0, Date Published: 2020-06-01T00:00:00-04:00, OSCAL Version: 1.0-Milestone3, Remarks: Updated for annual assessment.

Relevant Roles for this SSP
Prepared By(ID: prepared-by) - The organization that prepared this SSP. If developed in-house, this is the CSP itself.
Prepared For(ID: prepared-for) - The organization for which this SSP was prepared. Typically the CSP.
System Security Plan Approval(ID: contact-approver) - The individual or individuals accountable for the accuracy of this SSP.
Cloud Service Provider(ID: cloud-service-provider) - no description provided.
Information System Owner(ID: system-owner) - The individual within the CSP who is ultimately accountable for everything related to this system.
Authorizing Official(ID: authorizing-official) - The individual or individuals who must grant this system an authorization to operate.
Authorizing Official's Point of Contact(ID: authorizing-official-poc) - The individual representing the authorizing official.
Information System Management Point of Contact (POC)(ID: system-poc-management) - The highest level manager who responsible for system operation on behalf of the System Owner.
Information System Technical Point of Contact(ID: system-poc-technical) - The individual or individuals leading the technical operation of the system.
General Point of Contact (POC)(ID: system-poc-other) - A general point of contact for the system, designated by the system owner.
System Information System Security Officer (or Equivalent)(ID: information-system-security-officer) - The individual accountable for the security posture of the system on behalf of the system owner.
Privacy Officer's Point of Contact(ID: privacy-poc) - The individual responsible for the privacy threshold analysis and if necessary the privacy impact assessment.
Owner of an inventory item within the system (ID: asset-owner) - no description provided.
Administrative responsibility an inventory item within the system (ID: asset-administrator) - no description provided.
ICA POC (Local)(ID: isa-poc-local) - The point of contact for an interconnection on behalf of this system.
ICA POC (Remote)(ID: isa-poc-remote) - The point of contact for an interconnection on behalf of this external system to which this system connects.
ICA Signatory (Local)(ID: isa-authorizing-official-local) - Responsible for signing an interconnection security agreement on behalf of this system.
ICA Signatory (Remote)(ID: isa-authorizing-official-remote) - Responsible for signing an interconnection security agreement on behalf of the external system to which this system connects.
Consultant(ID: consultant) - Any consultants involved with developing or maintaining this content.
[SAMPLE]Unix Administrator(ID: admin-unix) - This is a sample role.
[SAMPLE]Client Administrator(ID: admin-client) - This is a sample role.
[SAMPLE]Program Director(ID: program-director) - This is a sample role.
Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO)(ID: fedramp-pmo) - no description provided.
Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB)(ID: fedramp-jab) - no description provided.

OSCAL Profile
Imported: #890170c3-04fa-4d25-a096-8e4070c237c

Control Implementation Details

ATLASITY Home Status Boards My Workbench News Feed Modules Calendar

Related Controls

Id: 1, PM: 9, PM: 24, PS: 0, SI: 12

Created By: Howerton, Travis

Date Created: 12-30-2020

Last Updated By: Howerton, Travis

Last Updated Date: 12-30-2020

Policy:
Statements
ac-1.stml.a
UUID: f64039a-dca7-44f5-9c17-6b343ee980c
Remarks: This identified component is the system itself. In any control implementation response that can not be associated with another component is associated with the component representing the system.
Components

Component ID	UUID	Description	Annotations
6092c0cf9353-4236-8003-2a5d417555fa	3f5612a4-c01d-4c47-dcae-75d2eaa332cd	Describe how Part a is satisfied within the system.	N/A

ac-1.stml.a.1
UUID: 0af60c0e-b5e5-4127-ae19-efb0d176775e
Remarks: This identifies a policy (attached in resources) that satisfies this control.
Links
(Type: policy)
(Link: #090ac0379-2009-4030-c9f0-260729e2e9)
ac-1.stml.a.2
UUID: f6f9e02-3058-400f00e6-3094e834a3f
Remarks: This identifies a process (attached in resources) that satisfies this control.
Links
(Type: process)
(Link: #ax-process-1)
ac-1.stml.b.1
UUID: 048f97ec-85c1-4249-9709-8a228f1e3791
Description: Describe how Part b-1 is satisfied.
ac-1.stml.b.2
UUID: 59c87969-305c-48f1-8a3e-1e642249633f
Description: Describe how Part b-2 is satisfied.

Annotations
Implementation-status: planned(Remarks: Describe the plan to complete the implementation.)
control-origination: spsystem

Control Owner: Howerton, Travis

Implementation:
Properties
planned-completion-date: 2020-11-27Z

Parameter Settings
ac-1.prm.1: {replace with list of personnel or roles}
ac-1.prm.2: {specify frequency}
ac-1.prm.3: {specify frequency}



Experiment 2 – Results MVP 2



Components

ATLASITY Home Status Boards My Workbench News Feed Modules Calendar howieavp

SECURITY PLAN FORM [Jump to Toolbar](#) [View Parent](#)

Basic Information Categorization Key Dates Description Stakeholders and Users **Components** Custom Fields

Components 4 [Add](#)

Actions	Title	Type	Status	UUID	Delete
View/Edit	AWS	software	Active	241704dd-78be-46cc-8542-51574711e45c	Delete
View/Edit	Drupal	software	operational	bba29c21-89bc-4201-9982-633334c2aad2	Delete
View/Edit	SSH	software	operational	af8b7ee0-e02f-424a-86f6-995c074f675f	Delete
View/Edit	This System	software	operational	5b43cd7a-22d8-4ad0-b70f-c2e45a10f6ec	Delete

Toolbar

[Save](#) [Delete](#) [Back](#) [Print](#) [Email](#) [Export](#) [Create New](#) [Jump to Top](#)

Security Plan Visualizer

Parameters

ATLASITY Home Status Boards My Workbench News Feed Modules Calendar howieavp

...
 {{9cb3d8fe-2127-48ba-821e-cdd2d7aee921}} - NIST Special Publication 800-100

Assessment Plan

- Assessment
 - Assessment Type: INTERVIEW
 - Organizational personnel with access control responsibilities organizational personnel with information security responsibilities

Parameters

UUID	Name	Value
1e61d0b8-09d0-4895-bb7d-eedfa1552fad	ac-1_prm_2	at least every 3 years
13af5f46-80c4-44b4-af2e-3f94dccba248	ac-1_prm_3	at least annually

Policy

Statements

ac-1_smt
 UUID: d3cedc53-16b8-4b1d-bc8d-67cff9b7c9cb
 Components

Component ID	UUID	Description	Annotations
5b43cd7a-22d8-4ad0-b70f-c2e45a10f6ec	88bb0430-446e-41cc-818a-3d32b507c919	Statement about AC-1	N/A

ac-1_smt.a
 UUID: 0ad4b106-9aec-48d0-a275-2090326b49fe
 Components

Control Owner *

Howerton, Travis (howieavp)

Implementation



Experiment 2 – Leveraged

SUCCESS

Parent Security Plan

The screenshot shows the 'SECURITY PLAN FORM' in the ATLASITY application. The form is for a system named 'NIST Master Plan' with ID # 49. It includes fields for 'System Name', 'Other Identifier', 'Status' (Operational), 'System Type' (General Support System), and 'Facility' (LANL). Key dates are 'Authorization Date: 01/15/2019' and 'Expiration Date: 01/15/2024'. The form is categorized as 'Moderate'. A toolbar at the bottom offers actions like Save, Delete, Back, Print, Email, Export, Create New, and Jump to Top. A 'Security Plan Visualizer' section is visible at the bottom of the form.

Leveraged Authorization

The screenshot shows the 'Security Plan Visualizer' for the 'NIST Master Plan'. It features four donut charts: 'CONTROLS BY STATUS' (Not Implemented), 'CONTROLS BY LAST ASSESSMENT RESULT', 'CONTROLS BY OWNER' (Howerton, Travis), and 'CONTROLS BY DATE LAST ASSESSED'. Below the charts is a 'Subsystems' section with a 'Compliance Explorer' and a 'Timeline' view. A table lists 'Control Implementations' (14) and 'Security Plans' (1). A table at the bottom shows one record for a security plan.

Actions	ID #	System Name	System Owner	Status	System Type	Categorization	Expiration Date
View	64	2 Twelve E3 Lab lab5	Howerton, Travis	Operational	General Support System	Moderate	



Learnings

- OSCAL standard is extremely robust and can structure huge amounts of content for efficient machine processing
 - Less than 1 week of total programming time to demonstrate these Proof of Concepts with Atlasity and OSCAL
- OSCAL allows for porting data between two separate vendor systems (GovReady and Atlasity)
 - Atlasity can now repeatably import any GovReady SSP via the OSCAL standard using automation
- Atlasity was able to quickly align to OSCAL Release Candidate (RC) nomenclature and constructs to demonstrate feasibility of these use cases providing data on readiness level for other vendors
 - Initial proof point for the broader vendor community
- Demonstrated leveraged authorizations using parent/child security plan relationships (native control inheritance) in Atlasity
 - Important for tiering security plans and for cloud service providers to break out cloud v/s customer responsibilities

Potential Next Steps

- Adding the ability to export SSPs, SAPs, SARs, Catalogs, and Profiles in OSCAL format from Atlasity – using Atlasity Community Edition as a [free OSCAL content publishing tool](#)
 - Provides the ability to quickly and easily generate OSCAL content
- Automating Security Assessment Plans (SAPs) and Security Assessment Reports (SARs)
 - Initial integration work has been performed to take automated scan results against DISA STIGS using the MITRE Heimdall tool to automate assessments in Atlasity
- Leveraging the Atlasity Issues module for managing Plans of Actions and Milestones (POAMs)
 - Automating tracking of security deficiencies from automated scanning and CDM tools
- Community feedback and sharing lessons learned with the NIST OSCAL and ATARC teams from this POC for continuous improvement
- Development of PIP or NPM packages for handling OSCAL content
 - Lower barrier of entry for adoption by tool vendors and other developers