



# Continuous, Automated Compliance with OSCAL

March 2nd, 2022

*Contact Information*

Conner Phillippi: [conner@secureframe.com](mailto:conner@secureframe.com)

Apostolos Delis: [apostolos@secureframe.com](mailto:apostolos@secureframe.com)

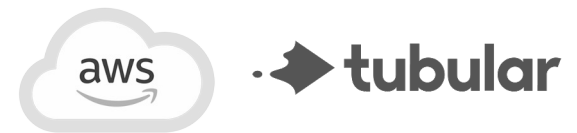
# About Us



**Conner Phillippi**  
Product



**Apostolos Delis**  
Engineering Lead



# Agenda



Introduction on  
Secureframe

Compliance  
Challenges

Secureframe Platform  
& OSCAL Applications

Group Q&A

# Intro on Secureframe

- Founded in January 2020
- Headquartered in San Francisco and Denver
- Automating security compliance for 500+ companies
- Helping customers stay secure, meet regulatory obligations, and break through customer & vendor security requirements
- Support SOC 2, ISO 27001, HIPAA, PCI DSS, CCPA, and GDPR compliance initiatives
- Entering the Federal compliance space in 2022 and will be able to support ANY framework

## Investors



## Clients





# Compliance Challenges

# Federal Compliance Challenges & Solutions

## Federal Challenges

- 1a Federal compliance & ATO reviews are complex, obscure, and costly for vendors
- 1b High federal compliance barriers cause a smaller pool of available vendors
- 2 Agencies are unable to truly monitor vendor compliance “continuously”
- 3 Internal compliance is tedious for agencies, especially when they are subjected to several compliance frameworks
- 4 Agencies struggle to objectively interpret controls and assess their implementation

## Secureframe Solutions

Simplify compliance requirements into an automated & actionable roadmap. Minimize vendor compliance readiness & audit costs. Validate SSPs to reduce time to ATO issuance.

Notify agencies in real-time when their authorized vendor(s) fail controls (as opposed to requesting static deliverables) with set tolerances.

Abstract all frameworks and controls via Secureframe and OSCAL. Push agencies to think in terms of security and risk rather than compliance to framework-specific controls.

Normalize NIST 800-53, HIPAA, PCI DSS, SOC 2, etc. compliance data via Secureframe and OSCAL; promote global control implementation consensus

# User Story A

## Continuously Assess Your Own Compliance



User

Government Agency or  
Private Sector Vendor



Goal

- Automatically assess internal framework compliance
- Output compliance data in a standardized format for ingestion by other vendors, agencies, and assessors

# 1. Connect GitHub Account

The screenshot displays the 'Integrations' section of the SecureFrame application. The left sidebar contains a navigation menu with items: Dashboard, Personnel, Asset Inventory, Policies, Vulnerabilities, Integrations (highlighted), Vendors, Vendor Access, Risk Management, Reports, and Data Room. The top right of the page shows the user's role as 'Working in Government Agency' and a profile picture. The main content area is titled 'Integrations' and has two tabs: 'CONNECTED INTEGRATIONS' (active) and 'AVAILABLE INTEGRATIONS'. A search bar is located below the tabs. Under 'Not Connected Integrations', there is a horizontal line. Under 'Connected Integrations', there are four entries, each with a logo, name, details, a 'SYNC' button, and a 'Connected' status with a green checkmark. A '+ ADD CONNECTION' button is present for each entry. A vertical 'Share feedback' button is on the right side of the integrations list.

| Integration | Account ID                           | Settings                 | SYNC                 | Last Sync           | Status    | Action                           |
|-------------|--------------------------------------|--------------------------|----------------------|---------------------|-----------|----------------------------------|
| AWS         | 257613929019                         | <a href="#">Settings</a> | <a href="#">SYNC</a> | Feb 23, 2022 6:03am | Connected | <a href="#">+ ADD CONNECTION</a> |
| Azure       | b74b0703-da3d-4db5-a1ff-79bbc0b2d679 |                          | <a href="#">SYNC</a> | Feb 23, 2022 6:15am | Connected | <a href="#">+ ADD CONNECTION</a> |
| GitHub      | Connection #1                        |                          | <a href="#">SYNC</a> | Feb 23, 2022 6:17pm | Connected | <a href="#">+ ADD CONNECTION</a> |
| Office 365  | 494c94e2-ce5c-439a-a14c-d59d76e4c151 |                          | <a href="#">SYNC</a> | Feb 23, 2022 6:32am | Connected | <a href="#">+ ADD CONNECTION</a> |



# 2. Configure GitHub Integration

The screenshot displays the Secureframe Asset Inventory interface. On the left is a dark sidebar with navigation options: Dashboard, Personnel, Asset Inventory (selected), Policies, Vulnerabilities, Integrations, Vendors, Vendor Access, Risk Management, Reports, and Data Room. The main content area is titled "Asset Inventory" and has tabs for COMPUTERS, CLOUD RESOURCES, and VERSION CONTROL. A search bar is present, and a table lists assets with columns for Provider and Repository Name. One asset is listed: Provider: Github, Repository Name: Secureframe-dev-demo/Backend.

An "Advanced Repository Settings" modal window is open, showing configuration options for the repository "Secureframe-dev-demo/Backend".

- Advanced Repository Settings**
  - Secureframe-dev-demo/Backend
  - Automate version control-related tests within Secureframe with the settings below. If you don't have a setting available, you can leave it blank and the associated test will default to a manual evidence upload.
  - Pull requests merged on or after February 22, 2022 will be evaluated in tests. This date can be changed [here](#).
  - Branches with production code**
    - Production branch name(s): main, release-v1.3
    - Please input all branches within this repository that contain production code.
  - Emergency label**
    - Emergency label: emergency
    - Apply to all in-scope repositories
  - Testing checks**
    - Integration test names: github-actions, dependabot
    - Apply to all in-scope repositories
    - Static code analysis test names: github-actions, dependabot
    - Apply to all in-scope repositories
    - Continuous dependency test names: dependabot
    - Apply to all in-scope repositories

The background interface shows a "Working in Government Agency" header, "REVIEW ASSETS" and "EXPORT CLOUD REPORT" buttons, a "Default Owner" dropdown set to "Apostolos Delis", and a table with columns "In Audit Scope" and "Owner". A "Share feedback" button is visible on the right edge.

# 3. Review Code Change Compliance Gaps

Working in Government Agency

## NIST Readiness Report

18 of 35 unique tests completed

REFRESH EXPORT...

Search

About this report

- Configuration Management 14 of 23 completed
- Audit and Accountability 3 of 10 completed
- Access Control 3 of 4 completed
- Identification and Authentication 2 of 4 completed

### CM-3 Configuration Change Control

a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled chan... [Show more](#)

12 TESTS

- Configurations for production servers
- Version control tools
- Pull request templates
- System patches
- Static analysis security testing (SAST)
- 1** Pull request approvals
- Dependency testing
- Integration testing
- 2** Branch merge request approvals

Share feedback

Government Agency configures its version control tool to require at least 1 independent approver prior to pull request entering production

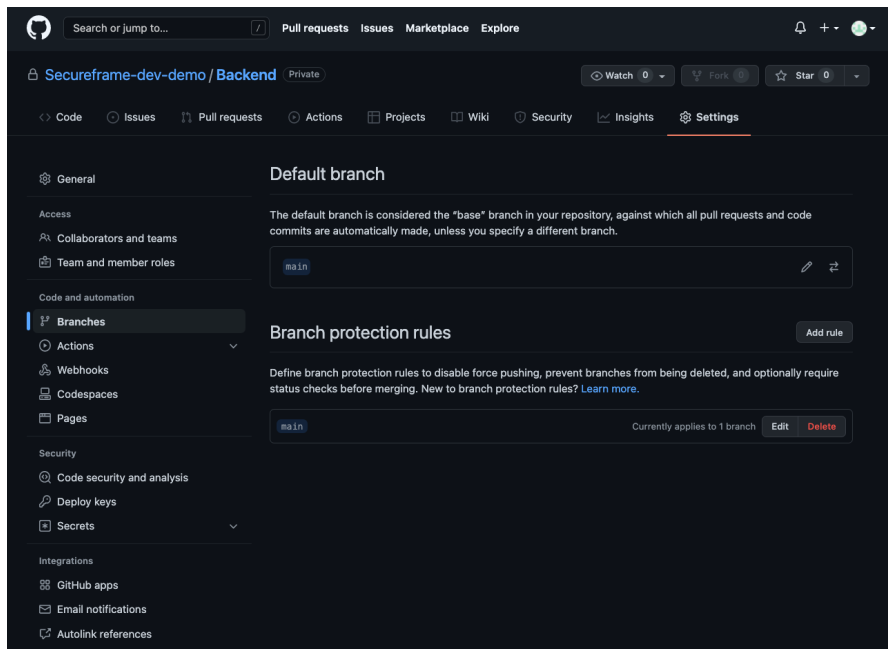
Branch "release-v1.3" from repository "Secureframe-dev-demo/Backend" is not configured to require merge request approvals

Government Agency requires branch merge requests to be independently reviewed and approved prior to merging to main, unless approved by an administrator due to a required emergency change

Pull request "Add 2.0 file" from repository "Secureframe-dev-demo/Backend" is not independently approved or labeled with an emergency label

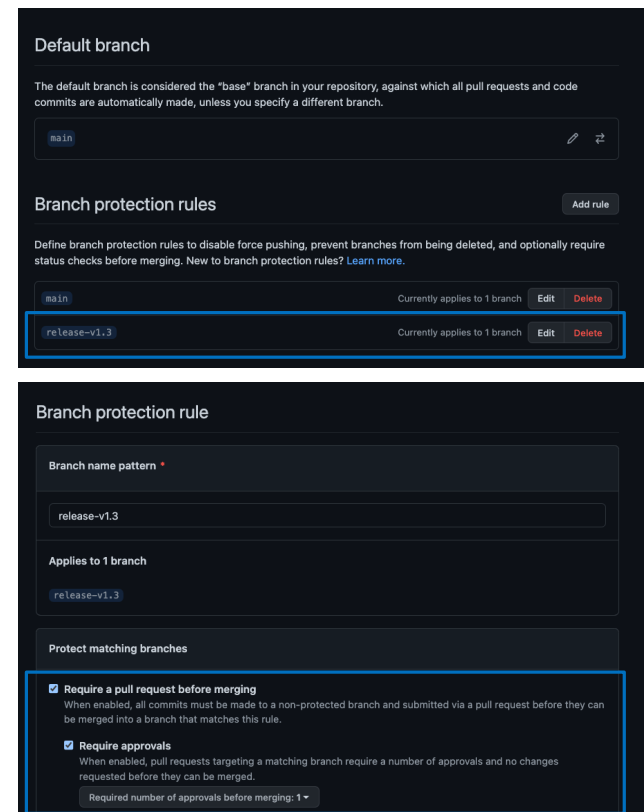
# 4a. Remediate Code Approval Gap

Branch “release-v1.3” is unprotected



The screenshot shows the GitHub repository settings for 'Secureframe-dev-demo / Backend'. The 'Branches' section is active, displaying 'Branch protection rules'. A table lists the 'main' branch with a status of 'Currently applies to 1 branch'. The 'release-v1.3' branch is not listed in this table, indicating it is not protected. A large grey arrow points from this screenshot towards the right-hand screenshot.

Branch “release-v1.3” is protected

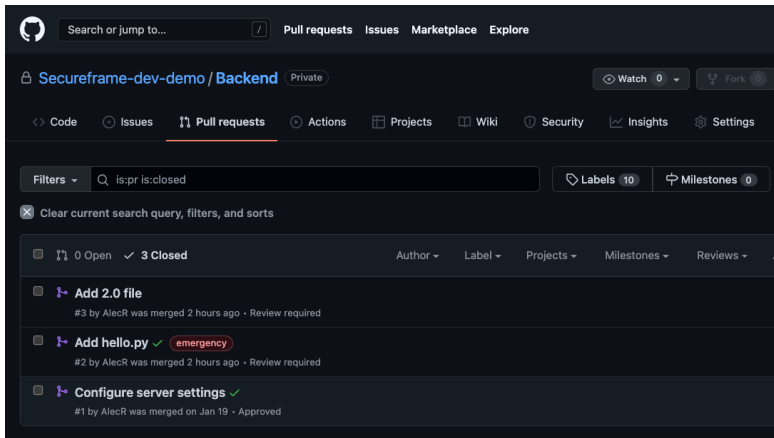


The screenshot shows the 'Branch protection rules' configuration for the 'release-v1.3' branch. The rule is highlighted with a blue border. It is configured with the following settings:

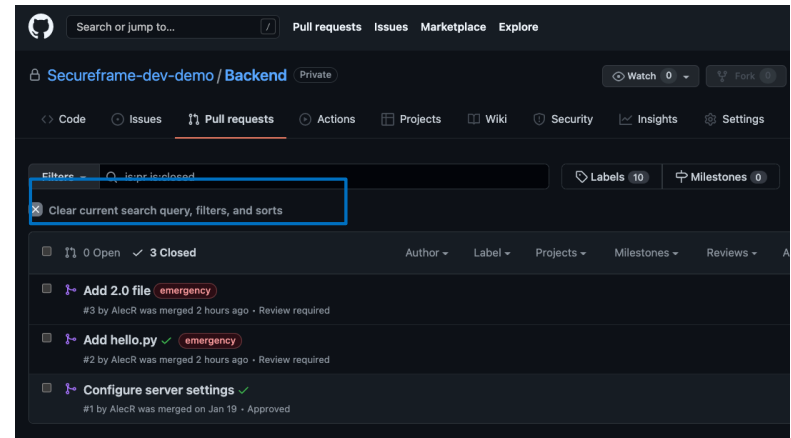
- Branch name pattern:** release-v1.3
- Applies to 1 branch:** release-v1.3
- Protect matching branches:**
  - Require a pull request before merging**  
When enabled, all commits must be made to a non-protected branch and submitted via a pull request before they can be merged into a branch that matches this rule.
  - Require approvals**  
When enabled, pull requests targeting a matching branch require a number of approvals and no changes requested before they can be merged.  
Required number of approvals before merging: 1

## 4b. Remediate Code Approval Gap

“Add 2.0 file” is missing approval/emergency label



“Add 2.0 file” is given emergency label



# 5. Secureframe Validates Remediations

Working in Government Agency

## NIST Readiness Report

20 of 35 unique tests completed REFRESH EXPORT...

Search

About this report

- Configuration Management 16 of 23 completed
- Audit and Accountability 3 of 10 completed
- Access Control 3 of 4 completed
- Identification and Authentication 2 of 4 completed

government\_agenc...  
Name Kind  
pull\_request\_approvals.csv Comma...et (.csv)

government\_agenc...  
Name Kind  
branch\_merg...approvals.csv Comma...et (.csv)

### CM-3 Configuration Change Control

a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; ... [Show more](#)

12 TESTS

- > Configurations for production servers
- Version control tools
- > Pull request templates
- > System patches
- Static analysis security testing (SAST)
- Pull request approvals
- Dependency testing
- Integration testing
- Branch merge request approvals
- > Code changes are tracked
- > Cloud infrastructure configuration changes are tracked
- > Segregated environments

1

2

Share feedback

government\_age...zip government\_age...zip Show All

# 6. Export API-Retrieved Evidence (.csv)

The image shows two screenshots of Excel spreadsheets. The top spreadsheet, titled 'pull\_request\_approvals', has columns A through J. Row 1 contains headers: Vendor, Repository, In Audit Scope, Branch Name, Required Approved Reviews Count, and Author Approval Enabled. Row 2 shows data for 'Github Secureframe-dev-demo/Backend' with 'In Audit Scope' set to TRUE and 'Branch Name' set to 'main'. Row 3 shows data for 'Github Secureframe-dev-demo/Backend' with 'In Audit Scope' set to TRUE and 'Branch Name' set to 'release-v1.3'. A green circle with the number '1' highlights the 'In Audit Scope' cell in row 3. The bottom spreadsheet, titled 'branch\_merge\_request\_approvals', has columns A through P. Row 1 contains headers: Vendor, Repository, Private Rep, Emergency Label, Has Label, Base Branch Name, Pull Request Name, Merged, Pull Request Author, and Independent App Opened At. Row 2 shows data for 'Github Secureframe-dev-demo/B' with 'Private Rep' set to TRUE and 'Emergency Label' set to 'emergency'. Row 3 shows data for 'Github Secureframe-dev-demo/B' with 'Private Rep' set to TRUE and 'Emergency Label' set to 'emergency'. Row 4 shows data for 'Github Secureframe-dev-demo/B' with 'Private Rep' set to TRUE and 'Emergency Label' set to 'emergency'. A green circle with the number '2' highlights the 'Private Rep' cell in row 4.

| Vendor | Repository                   | In Audit Scope | Branch Name  | Required Approved Reviews Count | Author Approval Enabled |
|--------|------------------------------|----------------|--------------|---------------------------------|-------------------------|
| Github | Secureframe-dev-demo/Backend | TRUE           | main         | 1                               | FALSE                   |
| Github | Secureframe-dev-demo/Backend | TRUE           | release-v1.3 | 1                               | FALSE                   |

| Vendor | Repository             | Private Rep | Emergency Label | Has Label | Base Branch Name | Pull Request Name         | Merged | Pull Request Author | Independent App Opened At |
|--------|------------------------|-------------|-----------------|-----------|------------------|---------------------------|--------|---------------------|---------------------------|
| Github | Secureframe-dev-demo/B | TRUE        | emergency       | FALSE     | main             | Configure server settings | TRUE   | AlecR               | 1 2022-01-19 1            |
| Github | Secureframe-dev-demo/B | TRUE        | emergency       | TRUE      | main             | Add hello.py              | TRUE   | AlecR               | 0 2022-02-24 0            |
| Github | Secureframe-dev-demo/B | TRUE        | emergency       | TRUE      | release-v1.3     | Add 2.0 file              | TRUE   | AlecR               | 0 2022-02-24 0            |

# 7. Export Report in OSCAL for Global Portability

The screenshot displays the NIST Readiness Report interface. At the top, it shows "Working in Government Agency" and a progress indicator for "20 of 35 unique tests completed". A search bar is visible on the left. The main content area lists various controls, including "Version control tools", "Pull request templates", "System patches", "Static analysis security testing (SAST)", "Pull request approvals", "Dependency testing", "Integration testing", "Branch merge request approvals", "Code changes are tracked", "Cloud infrastructure configuration changes are tracked", and "Segregated environments".

An "Export NIST Readiness Report" dialog box is open, asking "Which controls would you like to export?". The "OSCAL JSON" option is selected. Below the dialog, a file explorer window shows the following files:

| Name               | Kind |
|--------------------|------|
| oscal_catalog.json | JSON |
| oscal_profile.json | JSON |
| oscal_ssp.json     | JSON |

The interface also includes a "Share feedback" button on the right side.

# 8a. Reference (Catalog and Profile)

## Catalog

```
oscal_catalog.json  oscal_profile.json  oscal_ssp.json
No schema selected
1 {
2   "catalog": {
3     "uuid": "0c792c6c-5664-4c8c-98b4-cfb2b8b7e5fa",
4     "metadata": {
5       "title": "Government Agency System Security Plan for General Support System",
6       "published": "2022-02-24 04:36:12 UTC",
7       "last-modified": "2022-02-24 04:36:12 UTC",
8       "version": "v1.0",
9       "oscal-version": "1.0.1",
10      "roles": [
11        {
12          "id": "creator",
13          "title": "Document Creator"
14        },
15        {
16          "id": "contact",
17          "title": "Contact"
18        }
19      ],
20      "locations": [
21        {
22          "uuid": "0e048eaa-8b22-49cd-9ab0-1c8f71540579",
23          "title": "Government Agency Address",
24          "address": {
25            "type": "work",
26            "addr-lines": [
27              "1600 Pennsylvania Avenue NW"
28            ],
29            "city": "Washington",
30            "state": "DC",
31            "postal-code": "20500",
32            "country": "US"
33          },
34          "email-addresses": [
35            "usa@gov.com"
36          ]
37        }
38      ],
39      "parties": [
40        {
41          "uuid": "86c4742b-cae0-4f07-aaef-11330e46a483",
42          "type": "organization",
43          "name": "Government Agency LLC",
44          "email-addresses": [
45            "usa@gov.com"

```

## Profile

```
oscal_catalog.json  oscal_profile.json  oscal_ssp.json
No schema selected
107   "imports": [
108     {
109       "href": "./oscal_catalog.json",
110       "include-controls": [
111         {
112           "with-ids": [
113             "ia-2",
114             "cm-1",
115             "cm-3",
116             "cm-8",
117             "au-2",
118             "au-1",
119             "ac-1"
120           ]
121         }
122       ]
123     }
124   ],
125   "merge": {
126     "as-is": true
127   },
128   "back-matter": {
129     "back-matter": {
130       "resources": [
131         {
132           "uuid": "c3397cc9-83c6-4459-adb2-836739dclb94",
133           "title": "NIST Special Publication 800-53, Revision 5: * Security and
134             Privacy Controls for Information Systems and Organizations* (PDF)",
135           "rlinks": [
136             {
137               "href": "https://nvlpubs.nist.gov/nistpubs/SpecialPublications/
138                 NIST.SP.800-53r5.pdf",
139               "media-type": "application/pdf"
140             }
141           ]
142         }
143       ],
144       "rlinks": [
145         {
146           "href": "https://doi.org/10.6028/NIST.SP.800-53r5",
147           "media-type": "application/pdf"

```



# 8b. Reference (System Security Plan)

## Dynamic SSP Controls

```
oscal_catalog.json  oscal_profile.json  oscal_ssp.json
No schema selected
804 {
805   "uuid": "1ff2d4c2-bc9f-4408-8485-671e86694baa",
806   "control-id": "cm-3",
807   "remarks": "a. Determine and document the types of changes to the system
that are configuration-controlled; b. Review proposed configuration-
controlled changes to the system and approve or disapprove such changes
with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for
[cm-3_prm_1]; f. Monitor and review activities associated with
configuration-controlled changes to the system; and g. Coordinate and
provide oversight for configuration change control activities through
[cm-3_prm_2] that convenes [cm-3_prm_3]; when [cm-3_prm_4].",
808   "props": [
809     {
810       "name": "control-origination",
811       "ns": "https://secureframe.com/",
812       "value": "Service Provider System Specific"
813     },
814     {
815       "name": "implementation-status",
816       "ns": "https://secureframe.com/",
817       "value": "partial"
818     }
819   ],
820   "set-parameters": [
821     {
822       "param-id": "cm-3_prm_1",
823       "values": [
824         "at least 1 year"
825       ]
826     },
827     {
828       "param-id": "cm-3_prm_2",
829       "values": [
830         "change control meeting"
831       ]
832     },
833     {
834       "param-id": "cm-3_prm_3",
835       "values": [
836         "one or more times a month"
837       ]
838     },
839     {
840       "param-id": "cm-3_prm_4",
841       "values": [
842         "How changes require discussion or approval?"
843       ]
844     }
845   ]
846 }
```

## Dynamic SSP Assertions

```
oscal_catalog.json  oscal_profile.json  oscal_ssp.json
No schema selected
2276 {
2277   "statement-id": "cm-3_test_CM-8",
2278   "uuid": "3fe7f384-af8a-42eb-9a47-b77e751627a2",
2279   "props": [
2280     {
2281       "name": "test-status",
2282       "ns": "https://secureframe.com/",
2283       "value": "pass"
2284     },
2285     {
2286       "name": "enabled",
2287       "ns": "https://secureframe.com/",
2288       "value": "true"
2289     }
2290   ],
2291   "remarks": "{{company_name}} documents, tracks, and requires
independent approvals for material cloud infrastructure
configuration changes"
2292 },
2293 {
2294   "statement-id": "cm-3_test_CM-2",
2295   "uuid": "5138c8b1-9cb9-4c8d-a636-40761fa944b7",
2296   "props": [
2297     {
2298       "name": "test-status",
2299       "ns": "https://secureframe.com/",
2300       "value": "pass"
2301     },
2302     {
2303       "name": "enabled",
2304       "ns": "https://secureframe.com/",
2305       "value": "true"
2306     }
2307   ],
2308   "remarks": "{{company_name}} utilizes version control tools to govern
the code development cycle"
2309 },
2310 {
2311   "statement-id": "cm-3_test_CM-4",
2312   "uuid": "65dbb89f-c9fe-418e-b96d-73e1e44b4ec3",
2313   "props": [
2314     {
2315       "name": "test-status",
2316       "ns": "https://secureframe.com/",
2317       "value": "pass"
2318     },
2319     {
2320       "name": "enabled",
2321       "ns": "https://secureframe.com/",
2322       "value": "true"
2323     }
2324   ],
2325   "remarks": ""
2326 }
2327 }
```

## User Story B

# Monitor Vendor Compliance & Configuration Drift



User

Government Agency



Goal

- Inform vendor risk assessments & evaluations
- Automate configuration drift detection for vendors/CSPs

# 1. Select a Vendor for Evaluation (AWS)

The screenshot displays the 'Vendors' section of the Secureframe application. The interface includes a dark sidebar on the left with navigation options: Dashboard, Personnel, Asset Inventory, Policies, Vulnerabilities, Integrations, Vendors (highlighted), Vendor Access, Risk Management, Reports, and Data Room. The main content area features a header with the Secureframe logo, a user profile 'Working in Government Agency', and two buttons: '+ ADD VENDOR' and '+ UPLOAD CSV'. Below the header, there are tabs for 'ADDED VENDORS', 'SUGGESTED VENDORS', and 'ARCHIVED VENDORS', with 'ADDED VENDORS' selected. A search bar is present. The vendor list consists of six cards, each with a logo, name, and risk level:

| Vendor Name       | Risk Level        |
|-------------------|-------------------|
| AWS               | High Level Risk   |
| Azure             | High Level Risk   |
| Github            | High Level Risk   |
| Office 365        | High Level Risk   |
| Secureframe Agent | Medium Level Risk |
| Vetty             | High Level Risk   |

A 'Share feedback' button is located on the right side of the page.

## 2a. Upload Agency Baseline & AWS OSCAL Files

The screenshot displays the Secureframe AWS Vendor Management interface. A modal window titled "Upload Document" is open, showing the "OSCAL" tab. The modal contains two sections: "Reference JSON" and "Vendor JSON". Each section has a file input field and an "UPLOAD FILES" button. The "Reference JSON" section shows a file named "baseline\_oscsl\_json.zip". The "Vendor JSON" section shows a file named "amazon\_oscsl\_json.zip".

Two file selection windows are open, showing the contents of the selected files:

- The first window, titled "baseline\_oscsl\_json", contains a table with the following data:

| Name               | Kind |
|--------------------|------|
| oscsl_catalog.json | JSON |
| oscsl_profile.json | JSON |
| oscsl_ssp.json     | JSON |
- The second window, titled "amazon\_oscsl\_json", contains a table with the following data:

| Name               | Kind |
|--------------------|------|
| oscsl_catalog.json | JSON |
| oscsl_profile.json | JSON |
| oscsl_ssp.json     | JSON |

The background interface shows the "AWS Vendor Management" page with a sidebar on the left containing navigation options: Dashboard, Personnel, Asset Inventory, Policies, Vulnerabilities, Integrations, Vendors (selected), Vendor Access, Risk Management, Reports, and Data Room. The main content area displays the "Main Info" for the vendor, including fields for Company Name (AWS), Website (https://aws.amazon.com), Security URL (https://), Vendor Owner (Conner Phillippi), Services Provided (Cloud infrastructure, networking, storage and co), Date of Engagement (2022-02-28), Date of Last Review (2022-03-02), Authentication Type (Password, Single Sign-On), and Two Factor Enabled (toggle on). A "SAVE" button is visible at the bottom right of the main content area.

## 2b. Reference (Agency Baseline and AWS SSPs)

```
oscal_ssp.json
No schema selected
1 {
2   "system-security-plan": {
3     "uuid": "328988bc-9095-489b-bb62-2c0b6abd16b6",
4     "metadata": {
5       "title": "Baseline System Security Plan for General Support System",
6       "published": "2022-02-02 19:12:48 UTC",
7       "last-modified": "2022-02-02 19:12:48 UTC",
8       "version": "v1.0",
9       "oscal-version": "1.0.1",
10      "roles": [
11        {
12          "id": "creator",
13          "title": "Document Creator"
14        },
15        {
16          "id": "contact",
17          "title": "Contact"
18        }
19      ],
20      "locations": [
21        {
22          "uuid": "8e02a5be-2361-46ab-80d8-8240a30a0062",
23          "title": "Baseline Address",
24          "address": {
25            "type": "work",
26            "addr-lines": ["867 S VAN NESS AVE"],
27            "city": "SAN FRANCISCO",
28            "state": "CA",
29            "postal-code": "94110",
30            "country": "US"
31          },
32          "email-addresses": ["security@baseline.com"],
33          "phone-numbers": [
34            {
35              "type": "mobile",
36              "number": "2026416257"
37            }
38          ]
39        }
40      ],
41      "parties": [
42        {
43          "uuid": "ee836683-8903-41cb-9223-b37604ab0202",
44          "type": "organization",
45          "name": "Baseline, Inc.",
46          "email-addresses": ["security@baseline.com"],
47          "location-uuids": ["8e02a5be-2361-46ab-80d8-8240a30a0062"]
48        },
49        {
50          "uuid": "b075b10e-9819-4691-8bb2-2123417b4692",
51          "type": "organization",
52          "name": "Clearbit"
53        },
54        {
55          "uuid": "a4ddaec-5229-4a3b-9011-0d3add76529e",
56          "type": "organization",
57          "name": "Autopilot",

```

```
oscal_ssp.json
No schema selected
1 {
2   "system-security-plan": {
3     "uuid": "43523452-6455-fad3-342b-3252352da34f",
4     "metadata": {
5       "title": "Amazon Web Services System Security Plan for General Support System",
6       "published": "2022-02-02 19:12:48 UTC",
7       "last-modified": "2022-02-02 19:12:48 UTC",
8       "version": "v1.0",
9       "oscal-version": "1.0.1",
10      "roles": [
11        {
12          "id": "creator",
13          "title": "Document Creator"
14        },
15        {
16          "id": "contact",
17          "title": "Contact"
18        }
19      ],
20      "locations": [
21        {
22          "uuid": "a0a707c1-c7b0-4828-9663-d199d7f52f62",
23          "title": "Amazon Web Services Address",
24          "address": {
25            "type": "work",
26            "addr-lines": ["410 Terry Ave N"],
27            "city": "SEATTLE",
28            "state": "WA",
29            "postal-code": "98109",
30            "country": "US"
31          },
32          "email-addresses": ["security@amazon.com"],
33          "phone-numbers": [
34            {
35              "type": "mobile",
36              "number": "4084100962"
37            }
38          ]
39        }
40      ],
41      "parties": [
42        {
43          "uuid": "78e5579c-86ed-45bf-a91e-cf7cae034344",
44          "type": "organization",
45          "name": "Amazon COM LLC.",
46          "email-addresses": ["security@amazon.com"],
47          "location-uuids": ["8e02a5be-2361-46ab-80d8-8240a30a0062"]
48        },
49        {
50          "uuid": "c3419a7e-4e50-4094-ae2d-38dffcff3fc",
51          "type": "organization",
52          "name": "Zoom"
53        },
54        {
55          "uuid": "f3210d90-1a48-4825-97de-009c4421b4a2",
56          "type": "organization",
57          "name": "Unbounce"

```

# 3. Secureframe Creates a Diff of the Files

The screenshot displays the Secureframe Data Room interface. On the left is a dark sidebar with navigation options: Dashboard, Personnel, Asset Inventory, Policies, Vulnerabilities, Integrations, Vendors, Vendor Access, Risk Management, Reports, and Data Room (highlighted). The main content area is titled "Data Room" and shows a "FILES" tab with a search bar and buttons for "CREATE FOLDER", "UPLOAD FILES", and "EXPORT DATA". Below this, a breadcrumb path reads "Data Room > OSCAL Analysis" with a "DOWNLOAD ALL" button. A table lists files with columns for Name, Evidence Type, and Date Uploaded. One file is listed: "AWS-baseline-comparison-2022-02-03T20-10-29+00-00.json" with Evidence Type "Oscal Diff" and Date Uploaded "Feb 3, 2022". A "Share feedback" button is on the right. An overlay window titled "Downloads" shows a file explorer view of the same file, with columns for Name, Size (5 KB), Kind (JSON), and Date Added (Today at 6:24 PM). At the bottom, a taskbar shows the file name "AWS-baseline-c...json" and a "Show All" button.

| Name   | Evidence Type | Date Uploaded |
|--|---------------|---------------|
| <input checked="" type="checkbox"/> AWS-baseline-comparison-2022-02-03T20-10-29+00-00.json | Oscal Diff    | Feb 3, 2022   |

| Name  | Size | Kind | Date Added       |
|---|------|------|------------------|
| AWS-baseline-compariso...03T20-10-29+00-00.json | 5 KB | JSON | Today at 6:24 PM |

# 4. Review Control or Assertion Deviation

The image displays a comparison of two JSON configuration files in Visual Studio Code. The left pane shows the 'Agency CSP Baseline SSP' configuration, and the right pane shows the 'AWS SSP' configuration. A 'Diff' view on the right highlights differences between the two files.

**Agency CSP Baseline SSP**

```
2243 {
2244   "statement-id": "cm-3_test_CM-10",
2245   "uuid": "09030e59-0c18-4b36-8a87-2801d5823107",
2246   "props": [
2247     {
2248       "name": "test-status",
2249       "ns": "https://secureframe.com/",
2250       "value": "pass"
2251     },
2252     {
2253       "name": "enabled",
2254       "ns": "https://secureframe.com/",
2255       "value": "true"
2256     }
2257   ],
2258   "remarks": "{{company_name}} patches cloud service provider
2259   infrastructure and keeps respective systems and services up to date"
2260 },
2261 {
2262   "statement-id": "cm-3_test_SA-1",
2263   "uuid": "29740114-7e77-45ce-9614-303fbbbed8007",
2264   "props": [
2265     {
2266       "name": "test-status",
2267       "ns": "https://secureframe.com/",
2268       "value": "fail"
2269     },
2270     {
2271       "name": "enabled",
2272       "ns": "https://secureframe.com/",
2273       "value": "true"
2274     }
2275   ],
2276   "remarks": "{{company_name}} patches cloud service provider
2277   infrastructure and keeps respective systems and services up to date"
2278 },
2279 ]
```

**AWS SSP**

```
2238 {
2239   "statement-id": "cm-3_test_CM-10",
2240   "uuid": "09030e59-0c18-4b36-8a87-2801d5823107",
2241   "props": [
2242     {
2243       "name": "test-status",
2244       "ns": "https://secureframe.com/",
2245       "value": "fail"
2246     },
2247     {
2248       "name": "enabled",
2249       "ns": "https://secureframe.com/",
2250       "value": "true"
2251     }
2252   ],
2253   "remarks": "{{company_name}} patches cloud service provider
2254   infrastructure and keeps respective systems and services up to date"
2255 },
2256 {
2257   "statement-id": "cm-3_test_SA-1",
2258   "uuid": "29740114-7e77-45ce-9614-303fbbbed8007",
2259   "props": [
2260     {
2261       "name": "test-status",
2262       "ns": "https://secureframe.com/",
2263       "value": "fail"
2264     },
2265     {
2266       "name": "enabled",
2267       "ns": "https://secureframe.com/",
2268       "value": "true"
2269     }
2270   ],
2271   "remarks": "{{company_name}} patches cloud service provider
2272   infrastructure and keeps respective systems and services up to date"
2273 },
2274 ]
```

**Diff**

```
31 {
32   "uuid": "1ff2d4c2-bc9f-4408-8485-671e86694baa",
33   "control-id": "cm-3",
34   "description": "a. Determine and document the types of changes to the system that are
35   configuration-controlled; b. Review proposed configuration-controlled changes to
36   the system and approve or disapprove such changes with explicit consideration for
37   security and privacy impact analyses; c. Document configuration change decisions
38   associated with the system; d. Implement approved configuration-controlled changes
39   to the system; e. Retain records of configuration-controlled changes to the system
40   for [cm-3_prm_1]; f. Monitor and review activities associated with configuration-
41   controlled changes to the system; and g. Coordinate and provide oversight for
42   configuration change control activities through [cm-3_prm_2] that convenes
43   [cm-3_sys_3]; when [cm-3_prm_4]".
44   "implementation-status": "partial",
45   "failing-tests": [
46     {
47       "uuid": "09030e59-0c18-4b36-8a87-2801d5823107",
48       "test-id": "cm-3_test_CM-10",
49       "status": "fail",
50       "description": "{{company_name}} patches cloud service provider infrastructure
51       and keeps respective systems and services up to date"
52     }
53   ]
54 },
55 {
56   "uuid": "52d62724-2f2a-41a2-a2af-7e66adfad57e",
57   "control-id": "cm-8",
58   "description": "a. Develop and document an inventory of system components that: 1.
59   Accurately reflects the system; 2. Includes all components within the system; 3.
60   Does not include duplicate accounting of components or components assigned to any
61   other system; 4. Is at the level of granularity deemed necessary for tracking and
62   reporting; and 5. Includes the following information to achieve system component
63   accountability: [cm-8_prm_1]; and b. Review and update the system component
64   inventory [cm-8_prm_2].",
65   "implementation-status": "partial",
66   "failing-tests": [
67     {
68       "uuid": "654ad1f1-9f06-4280-aff4-46e53ab49b2f",
69       "test-id": "cm-8_test_AM-3",
70       "status": "fail",
71       "description": "{{company_name}} maintains an inventory of production version
72       control repositories"
73     }
74   ]
75 },
76 {
77   "uuid": "da713515-a645-4f5a-86cf-59de39148b9c",
78   "control-id": "au-2",
79   "description": "a. Identify the types of events that the system is capable of logging
```



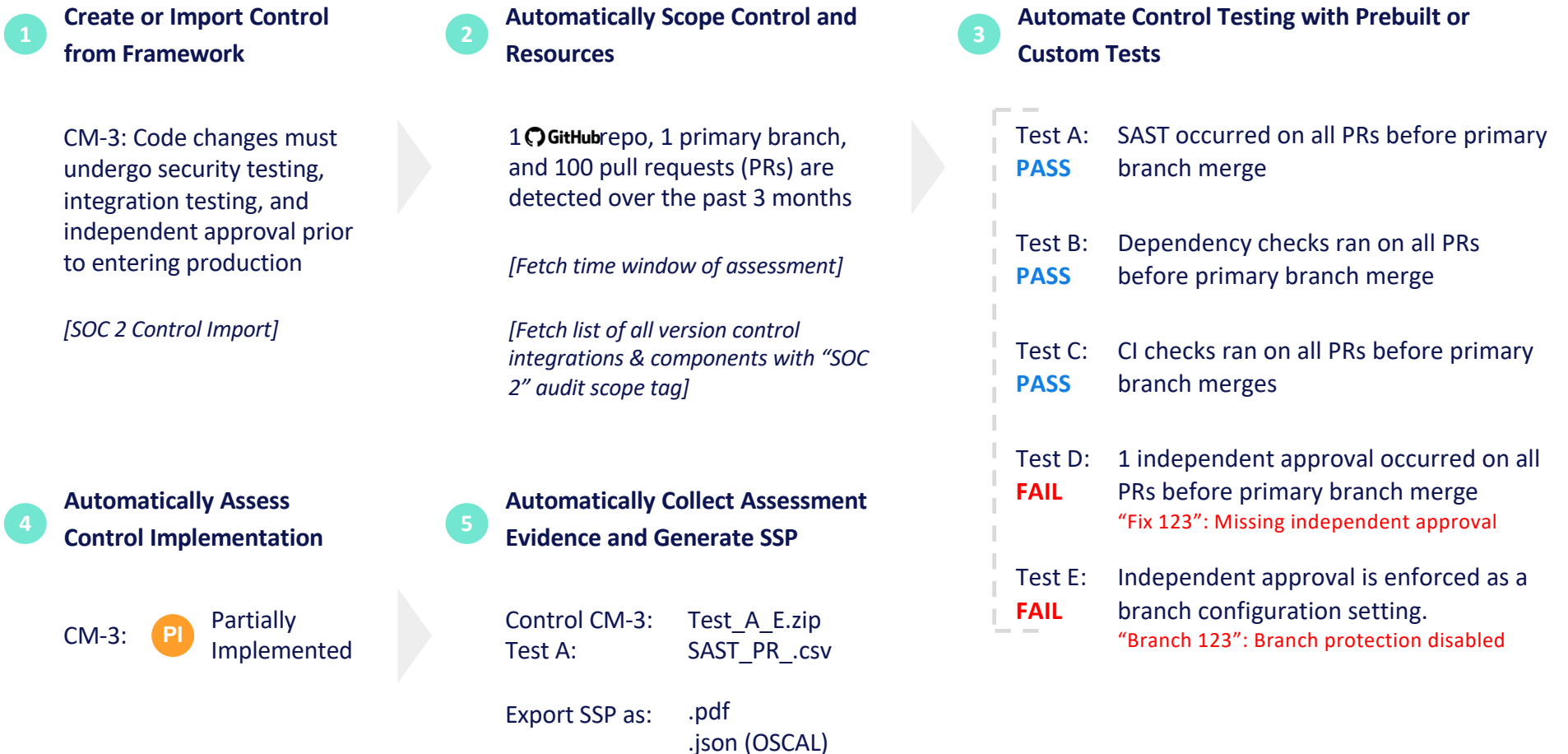
# Group Q&A

*Questions or Inquiries? Contact us at [oscal@secureframe.com](mailto:oscal@secureframe.com)*



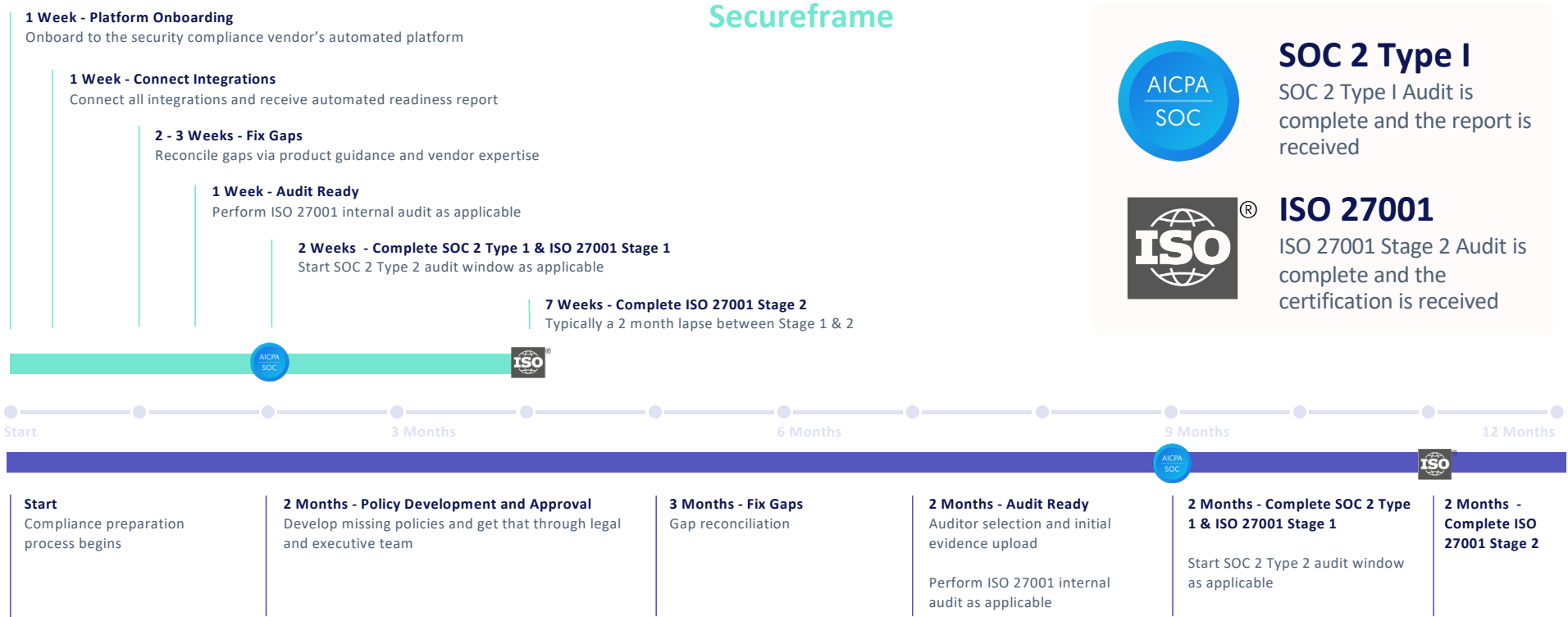
# Appendix

# How It Works: Control Assessment



# Commercial Compliance Time Savings

## Secureframe



**SOC 2 Type I**  
SOC 2 Type I Audit is complete and the report is received



**ISO 27001**  
ISO 27001 Stage 2 Audit is complete and the certification is received

## No Automation

# General Challenges of the Compliance Process

- 1. Collecting Audit Evidence is Manual & Time Consuming**
  - Internal applications do not automatically communicate with the auditing applications & process
  - Hundred screenshots are required in this process
- 2. Maintaining Compliance Eats into Other Company Initiatives** — With the amount of cross-functional work required to initially complete and continuously maintain compliance, primary company initiatives are often impeded
- 3. Understanding Compliance Requirements is Hard** — Compliance is a blackbox industry. Having guidance and direction is key for implementing the correct policies, technology, and internal processes.

