

EVERYONE'S GUIDE TO THE CCPA

Using the

NIST TM

PRIVACY FRAMEWORK

**To audit CCPA compliance according
to NIST 800-53 control standards**

"TM: a Registered Mark of NIST, which does not imply product endorsement by NIST or
the U.S. Government."

NIST Privacy
Framework Resource
contributed by



Privacy Portfolio

Authored by Craig Erickson, a California Consumer

August 2023

"EVERYONE'S GUIDE TO THE CCPA" is a tool for understanding the Regulations, building Privacy Programs, assessing legal compliance, privacy risks, and evidence gathered for mandated cybersecurity audits.

Formatted as an Excel Workbook, it is used by all stakeholders to determine whether a company deemed a "high-risk processor" should be subject to cybersecurity audits mandated by the CPRA-amended CCPA.

"EVERYONE'S GUIDE" contains self-assessment questions for evaluating respondents' understanding of the law and tests which generate evidence to fulfill regulatory requirements.

The CCPA Guidelines are represented by Statute, Section Title, and Paragraph, and are organized according to CCPA Test Suites.

Overview

- I. CCPA Compliance Test Suite**
220 CCPA test cases are derived from CCPA Final Regulations.
- II. NIST 800-53r5 Control Set**
Each CCPA test case is evaluated by 800-53r5 control standards.
- III. NIST Privacy Framework Methodology**
Each CCPA test case uses NIST Privacy Framework functions and tasks to design and evaluate 800-53r5 controls.
- IV. Risk Assessments & Cybersecurity Audits Mandated By the California Privacy Protection Agency**
Each CCPA test case result produces evidence for risk assessments and audits required by enforcement agencies.

NIST Privacy
Framework Resource
contributed by



Privacy Portfolio

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

Everyone's Guide to the CCPA is also used for:

- **Privacy Program Management:** The CCPA self-assessment can garner participation across functional teams and distribute work items relevant to each members' roles and goals to meet selected goals or to build comprehensive programs.
- **Security and Audit Controls:** Each CCPA legal compliance requirement can be mapped to NIST 800-53r5 control standards to leverage existing controls or implement new controls for underlying data security and privacy protections which support CCPA legal compliance requirements and provide evidence for mandatory cybersecurity audits.
- **Vendor Risk Management:** Each CCPA legal compliance requirement can be mapped to test cases applied to each vendor's products and services. These test cases are designed to be executed by any stakeholder, including consumers and enforcement agencies, to verify self-assessment responses, and produce evidence for underlying data security and privacy protections in support of the CCPA.

CCPA Compliance Test Suite

1. Verification

Verifying the identity of a consumer is a security prerequisite for fulfilling CCPA access requests.

2. Opt-out

Opting-out is a popular but difficult-to-implement CCPA provision.

3. Restrictions On Collection And Use

Restricting the collection and use of personal information is one of the best methods for reducing CCPA-compliance risks.

4. Limit

Limiting how specific elements of personal information are processed is an example of good data governance practices.

5. Third Parties

Enforcing CCPA legal obligations through contracts with external supply-chain partners requires strong vendor risk practices.

6. Access Requests

"Data Subject Access Requests" or DSARs, represent how California Consumers can exercise their CCPA rights.

7. Disclosures

Disclosing what personal information is collected and for which purposes is a core CCPA requirement.

8. Enforcement

Enforcing CCPA requirements is a shared responsibility among businesses, consumers, and enforcement agencies.

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

CCPA Test Suites are not prescriptive; they are designed to evaluate how well various legal strategies or technical risk controls perform in the pursuit of achieving specific compliance goals.

Verification

General Rules Regarding Verification.

Verification for Password-Protected Accounts.

Verification for Non-Accountholders.

Identity Access Control mechanisms can be designed for authenticating and authorizing access for all users in accordance with role-based, context-sensitive access control policies and procedures.

LINK to all	Questionnaire	Section Title	Subdivision	Description	Standard	Guidance	Exception	ISSUE	Remediation	Remediation Example	Test Case Title	ROLES	GOAL OR STRATEGY
11 Test cases	Which method is used to verify the identity of a consumer?	General Rules Regarding Verification.	(a)	(a) A business shall establish, document, and comply with a reasonable	i. reasonable	§ 7001. Definitions. (mm) "Verify" means to determine that	[none]	Non-Compliant Verification Procedures	Update Verification Procedures	Search OAG.ca.gov website for 'unreasonable' AND	Method For Verifying	Privacy, Legal, PM, Analyst, Security, Vendor Risk, HR	Identify Method to Verify Consumer's Identity

Final Guidelines issued by the California Privacy Protection Agency (CPPA) provided Guidance, Issues, Remediations, and Remediation Examples. "EVERYONE'S GUIDE" helps translate legal requirements into constructive actions for every stakeholder.

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

Although employees and job applicants are included as California Consumers, there is little regulatory guidance available at this time.

ROLES	CCPA TITLES	GOALS	QUESTIONNAIRE	CCPA TEST CASES
HR Human Resources are responsible for consumer data of employees and job applicants, which include sensitive information used in background checks, health and financial benefit programs, and internal investigations.	Section A. Estimated Private Sector Cost Impacts	Identify Annual (Estimated) Revenue	How many employees does your business have?	Minimum Revenue Threshold
	Training.	Communicate CCPA Requirements and Procedures to Responsible Staff	How many individuals on staff are responsible for handling consumer inquiries or complying with the CCPA are informed of all of the requirements in the CCPA and these regulations?	Trained Staff
		Identify Special Training Requirements	Is your firm required to document and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA are informed of all of the requirements in the CCPA and these regulations?	Special Requirements
1. SELECT YOUR ROLE	2. SELECT YOUR AREA	3. SELECT YOUR GOAL	4. ASSESS COMPLIANCE RISK	5. TEST RESIDUAL RISK

In many companies, only a few employees are aware of their company's legal status or annual revenue regarding CCPA exemptions.

EVERYONE’S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

CCPA case law contains Definitions, Standards, Exceptions, Exemptions, and Prerequisites which do not apply to all types of organizational entities and classes of individual consumers. CCPA Test Cases address different approaches, instances, and conditions, for each stakeholder role.

**The CCPA Test Suite consists of tests for each use case,
at different stages in the development lifecycle process,
for each specific stakeholder role seeking to achieve their own objectives,
within the context of helping consumers exercise their CCPA rights,
fulfilling CCPA compliance obligations,
and assessing independently verified and validated test results.**

Demonstration:

"I am a Developer, and I want to protect sensitive personal information from being improperly shared."

"I am a Product and Marketing Director who wants to avoid unnecessary requirements that could cause additional expense and delays in our product launch."

"I am a Consumer who wants to know if my vendor is a high-risk CCPA-covered entity."

"I am a Third-party Privacy Consultant providing privacy-preserving products, services, and advice to businesses, and my clients need to know if our firm's solutions comply with the CCPA."

"I am an Enforcement Agency investigating a complaint regarding a business' privacy and security practices, and I want to discover similar violations with other relevant laws."

"I am a Data Broker registered with the State of California who wants to assess if my security and privacy risk controls support CCPA-compliant business practices."

"I am a Vendor Risk Manager, and I want to know if my suppliers are violating the contract terms required by the CCPA."

"I am a Third-party Auditor who wants to know how many CCPA requirements are met using existing NIST controls."

"I am an Authorized Agent for consumers who want to report CCPA violations in complaints or incident reports to appropriate enforcement agencies."

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

ROLES	CCPA TITLES	GOALS	QUESTIONNAIRE	CCPA TEST CASES
Audit Represents internal or external auditors responsible for responding to mandated cybersecurity audits, investigations, or complaints received or initiated by an Agency.	Record-Keeping.	Maintain Required Records	What is the retention period for records of consumer requests made?	Records Integrity
		Maintain Required Information in Records	Do your records include how the business responded to consumer requests?	Request-Response Categories
		Maintain Reasonable Security for Records	What reasonable security procedures and practices are used to maintain these records?	Deidentification, Encryption, Access
		Identify Format for Maintaining Records	In what format(s) are the records maintained?	Record-keeping Sources
		Identify Access Control to Records	Which person(s) or Role(s) has access to these records?	Non-Compliant Record Sharing
		Maintain Minimum Data Retention of PI	Is personal information retained solely for the purpose of fulfilling a consumer request?	Requirement to Retain PI

Here we have one legal requirement for all CCPA-covered entities, which doesn't concern other roles outside of Legal and Privacy within the organization, but has counterparts outside the organization, such as Agencies, Consumers, Authorized Agents, and Service Providers, Contractors, and Third Parties.

It's often helpful to organize "minimal requirements" for each stakeholder role.

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

1. SELECT YOUR ROLE	2. SELECT YOUR AREA	3. SELECT YOUR GOAL	4. ASSESS COMPLIANCE RISK	5. TEST RESIDUAL RISK	6. METHODOLOGY USED	7. COMPOSE USER STORY
Auditor	Agency Audits.	Maintain History of Compliance	Can the Agency conduct an audit if your business has a history of noncompliance with the CCPA or any other privacy protection law?	Evidence of Compliance	[choice]	[context]
<p>As an internal or external auditor, I use objective, evidence-based findings to evaluate risks to the business, including legal compliance, and the security and safety to the public.</p> <p>To fulfill my mission, I use the tools and techniques used by Enforcement Agencies to evaluate privacy and security practices, so any discrepancies can be understood and resolved.</p>					6.a. QUESTIONNAIRE ONLY	I have evidence of compliance which may contradict or offset any violations of privacy laws. My access to agency complaints or legal correspondence is limited.
					6.b. QUESTIONNAIRE & TEST	I have evidence of compliance which may contradict or offset any violations of privacy laws. I executed the appropriate control tests and did not find evidence that would support agency complaints or determination of high-risk activities.
					6.c. TEST & QUESTIONNAIRE	I'm not aware of all applicable laws so I executed test cases to generate the correct response.
					6.d. NIST 800-53r5 CONTROLS	I'm using evidence of existing NIST 800-53 controls to prove our History of Compliance.
					6.e. NIST Privacy Framework Core	We have mixed levels of maturity for different control domains, so we select the appropriate Privacy Framework functions.
					6.f. NIST Privacy Framework Task, Knowledge, & Skill Statements	We align Task, Knowledge, and Skill Statements with CCPA Goals to distribute work among the team.
					6.g. NIST Privacy Framework PRAM	We use the Privacy Risk Assessment Method to identify, govern, communicate, control, and protect PI from adverse risk events.

Can CCPA Compliance Test Cases Be Evaluated According to NIST 800-53r5 Control Standards?

NIST SP 800-53r5 Control Set

Maximum limit of 100 controls arbitrarily set to reduce complexity.

Different control categories can be selected using the Privacy Framework, and specific control enhancements can be substituted for control categories to tailor NIST controls to suit your environment.

These controls were selected for their “privacy-preserving” qualities, alignment with common controls from ISO, CIS, and NIS 2, and crosswalk mappings to the Cybersecurity Framework and Privacy Framework.

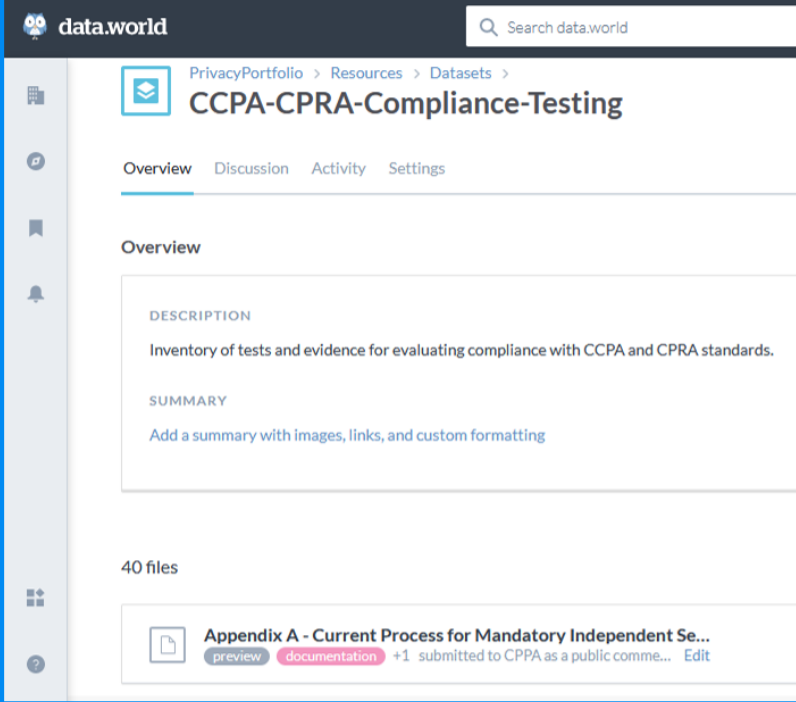
This control set supports the California Privacy Protection Agency’s goal of re-using existing cybersecurity and compliance controls for Mandatory CCPA Cybersecurity Audits.

Originally, NIST Privacy Framework Categories were mapped to the CCPA sections, but there is no one-to-one relationship between a CCPA test case and a Privacy Framework function, category or subcategory.

Almost every CCPA test case result produces evidence of compliance with multiple 800-53r5 controls in this set.

Risk Assessments & Cybersecurity Audits Mandated By the CPPA

CPPA Public Comments: Preliminary Rulemaking Activities on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking



The screenshot shows the 'data.world' interface. At the top, there's a search bar and navigation links for 'PrivacyPortfolio', 'Resources', and 'Datasets'. The main title is 'CCPA-CPRA-Compliance-Testing'. Below the title are tabs for 'Overview', 'Discussion', 'Activity', and 'Settings'. The 'Overview' tab is selected. It contains a 'DESCRIPTION' section with the text 'Inventory of tests and evidence for evaluating compliance with CCPA and CPRA standards.' and a 'SUMMARY' section with the text 'Add a summary with images, links, and custom formatting'. Below these sections, it says '40 files'. At the bottom, there's a file preview for 'Appendix A - Current Process for Mandatory Independent Se...' with a 'preview' button and a 'documentation' button. A note indicates '+1 submitted to CPPA as a public comment' and an 'Edit' button.

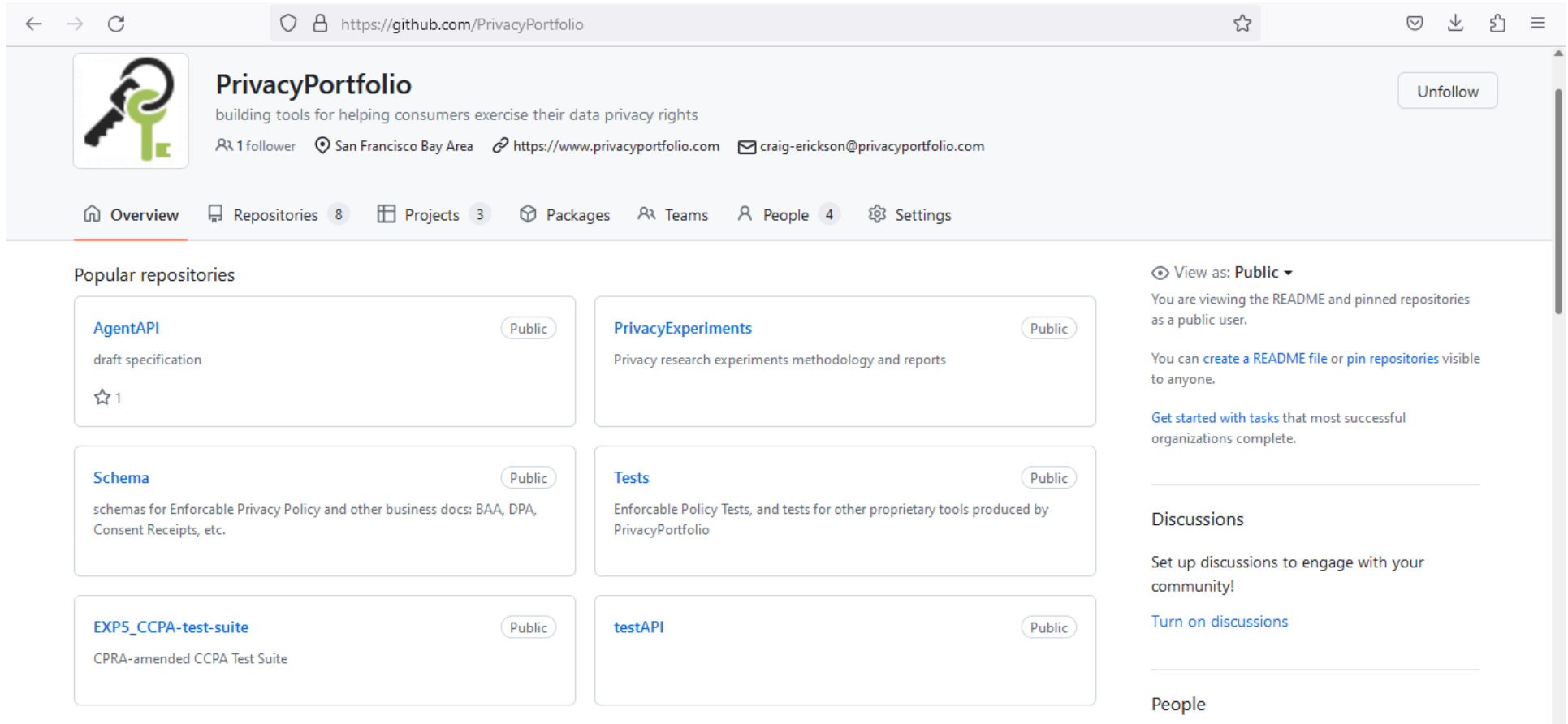
Test results published in my data catalog
can be reviewed by consumer, vendor, or agency.

Legal compliance implies the existence of adequate technical and administrative controls.

NIST 800-53r5 control tests for cybersecurity and data protection generate evidence in support of CCPA Test Cases.

NIST controls AND the CCPA test cases apply to *instances of compliance*, such as *for each vendor, product, or process*, rather than overall compliance for the entire organization.

Where is the code for automating these CCPA Test Cases?



The screenshot shows the GitHub profile for PrivacyPortfolio. The header includes the repository name, a description 'building tools for helping consumers exercise their data privacy rights', and contact information. Below the header is a navigation bar with links to Overview, Repositories (8), Projects (3), Packages, Teams, People (4), and Settings. The main content area is titled 'Popular repositories' and displays a grid of six repositories: AgentAPI (draft specification, 1 star), PrivacyExperiments (Privacy research experiments methodology and reports), Schema (schemas for Enforcable Privacy Policy and other business docs: BAA, DPA, Consent Receipts, etc.), Tests (Enforcable Policy Tests, and tests for other proprietary tools produced by PrivacyPortfolio), EXP5_CCPA-test-suite (CPRA-amended CCPA Test Suite), and testAPI. On the right side, there is a 'View as: Public' dropdown, a note about viewing the README and pinned repositories, a link to create a README file or pin repositories, a section for discussions with a link to turn on discussions, and a section for people.

PrivacyPortfolio
building tools for helping consumers exercise their data privacy rights
1 follower San Francisco Bay Area <https://www.privacyportfolio.com> craig-erickson@privacyportfolio.com

Overview Repositories 8 Projects 3 Packages Teams People 4 Settings

Popular repositories

- AgentAPI** (Public)
draft specification
★ 1
- PrivacyExperiments** (Public)
Privacy research experiments methodology and reports
- Schema** (Public)
schemas for Enforcable Privacy Policy and other business docs: BAA, DPA, Consent Receipts, etc.
- Tests** (Public)
Enforcable Policy Tests, and tests for other proprietary tools produced by PrivacyPortfolio
- EXP5_CCPA-test-suite** (Public)
CPRA-amended CCPA Test Suite
- testAPI** (Public)

View as: Public ▼
You are viewing the README and pinned repositories as a public user.
You can [create a README file](#) or [pin repositories](#) visible to anyone.
[Get started with tasks](#) that most successful organizations complete.

Discussions
Set up discussions to engage with your community!
[Turn on discussions](#)

People

An important design goal is having tests that can be reproduced by different stakeholders – including consumers.

Specific tests can also be found from other sources, such as W3C.org for testing the validity of GPC signals, Consumer Reports for testing digital ads, etc.

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

Assigning NIST controls to privacy laws isn't a common practice. The Privacy Framework was used to develop these tests and to bridge the gap between privacy and security teams. This example demonstrates how the "Matching Method" is defined by law, and detects compliance gaps in other areas, such as Vendor Risk, in which a third party provides the verification service, without the business knowing which method is used, and to what degree of accuracy.

NIST Privacy Framework Methodology

FUNCTION
IDENTIFY-P (ID-P)
Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

CATEGORY
Inventory and Mapping (ID.IM-P):
Data processing by systems, products, or services is understood and informs the management of privacy risk.

SUBCATEGORY
ID.IM-P1: Systems/products/services that process data are inventoried.

CCPA Section Title: General Rules Regarding Verification.

CCPA Section Title Description: (c) In determining the method by which the business will verify the consumer's identity, the business shall: (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

CCPA Test Case Title: Matching Method

CCPA Test Case Issue: Failure to Match Identifying Information Provided By Consumer

CCPA Test Case Guidance: (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themselves before deleting, correcting, or disclosing the consumer's data.

Question: "Is the Matching Method used by a third-party identification service to verify the identity of a consumer?"

My expectation as a Consumer, is that if a verification service is used, it should be listed as a "trusted third-party" or include a proper disclosure before sending the user to another domain where personal information is collected. Because there is no single, absolute standard for identity-proofing individual persons, tests are needed to inform stakeholders as to what the privacy risks are, for evaluation on a case-by-case basis.

EVERYONE’S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

A CCPA-covered business uses Privacy Framework Task, Knowledge, and Skill Statements mapped to Privacy Framework Core Outcomes.

The business is an Authorized Agent using a storage vendor within a Zero-Trust Environment to access and share personal data of consumers.

NIST Privacy Framework Methodology

TASK

Task T113 Maintain system or data store for inventory information.

KNOWLEDGE

Knowledge K036 Knowledge of inventory options and tools (e.g., Configuration Management Databases, Information Technology Service Management tools).

SKILLS

Skill S061 Skill in querying inventory management systems.

Task, Knowledge, and Skill Statements for each subcategory are used to translate policy and legalese into operational workstreams for cross-functional team roles.

Our Inventory System

1. ByOwner (customer, consumer, vendor, department, employee, application);
2. ByQuery (database, API);
3. ByResource (container, resource group, storage);
4. ByTag (label, metadata, access);
5. ByEvent (log, trigger, alert).

We use Dropbox to share personal information between consumers and the organization through Shared Folders the consumer has partial control of.

Inventory Metadata

1. Owners of Dropbox folders and files are documented in properties and event logs;
3. Dropbox storage is segmented by folders, files, and access permissions;
4. Labels and tags are applied to Dropbox folders, files, and access;
5. Dropbox event logs document creation, modification, sharing, and deletion of folders and files.

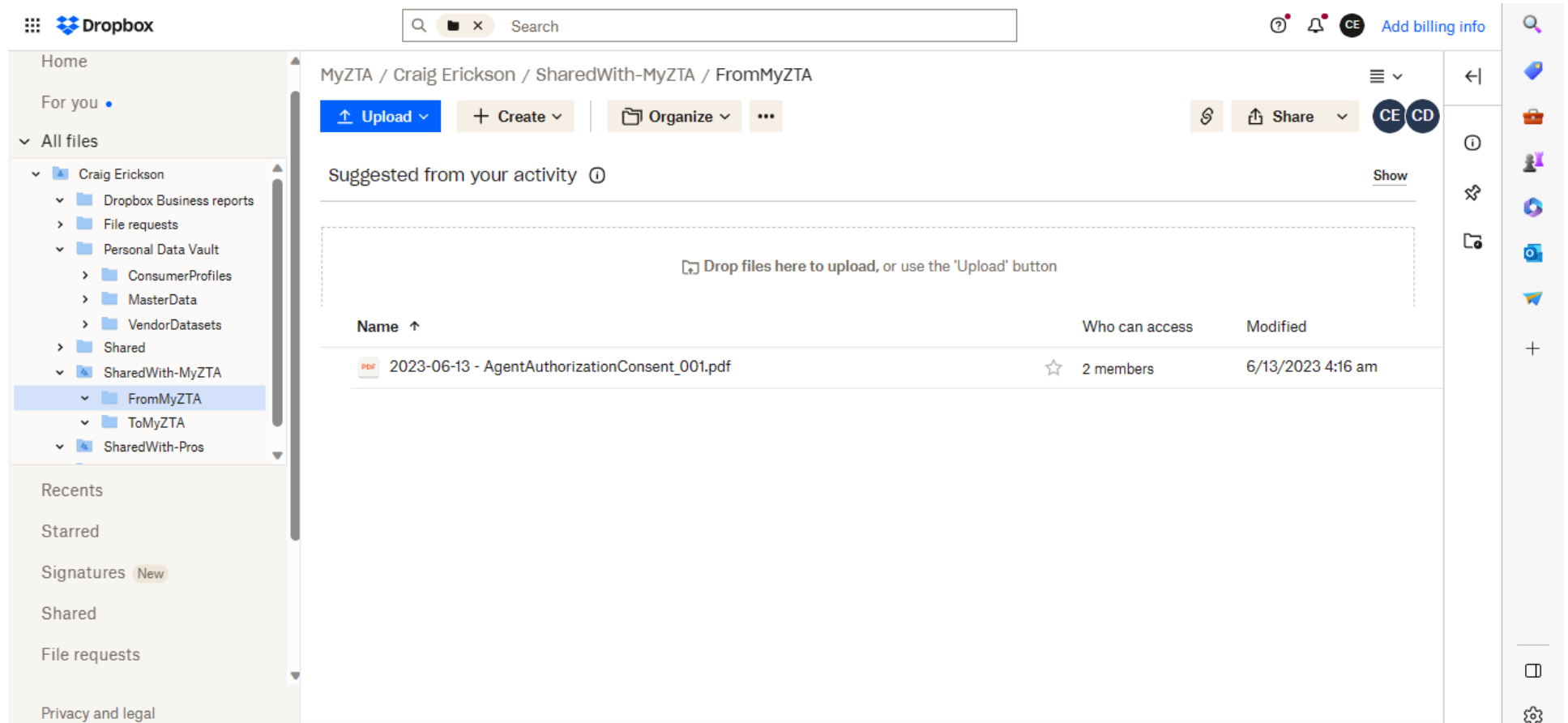
CCPA Compliance Goals are mapped to Task, Knowledge and Skill Statements, facilitated by keywords, “Identify”, “Communicate”, “Control”.

“Maintain” keyword maps to Governance and Protect functions of the Privacy Framework Core.

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

This screenshot shows how the Authorized Agent uses Dropbox to govern the Consumer's personal information:



Dropbox supports the needs of businesses AND consumers, and was selected as a preferred vendor due to its account management portal featuring robust customer-configurable security and privacy preferences, all of which can be tested according to NIST 800-53r5 control standards.

Vendor tests are not publically available. They are shared only with the vendor and an enforcement agency if a consumer complaint is filed.

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

One Dropbox feature is called "Who viewed my files?". To test it properly, we also need to test access control to make sure we aren't missing any paths for exfiltration to unaccounted-for users. APIs help automate the testing and reporting of results.

The screenshot shows the Azure DevOps interface for a test case. The breadcrumb navigation at the top reads: Azure DevOps / craigericksondp / test plans / Test Plans / DropBox. The test case is titled 'TEST CASE 3' and '3 dropbox.com_account-access_1'. It is created by 'Craig Erickson' and has '1 comment' and an 'Add tag' button. The 'State' is 'Design' and the 'Area' is 'test plans'. The 'Reason' is 'New' and the 'Iteration' is 'test plans\Sprint 1'. The 'Description' section includes reference sources: [Account access - Dropbox Help](#), [HTTP - Developers - Dropbox](#), and [Dropbox API Explorer](#). An example of a URL is provided in a light blue box: `https://api.dropboxapi.com/2/users/features/get_values`. The description continues with the text: 'for a given account, verify the available features before testing.' and 'next:'. A list of five test steps follows: 1. "What are all the ways I can access this account?", 2. "What are all the ways I can block myself from accessing this account?", 3. "What types of access can I give to others?", 4. "How can I revoke access given to others?", and 5. "How can I see who accessed this account?". At the bottom, there are checkboxes for 'account-access/acc' and 'organize/move'.

TEST CASE 3

3 dropbox.com_account-access_1

Craig Erickson 1 comment Add tag

State Design Area test plans

Reason New Iteration test plans\Sprint 1

Description

reference sources: [Account access - Dropbox Help](#), [HTTP - Developers - Dropbox](#), [Dropbox API Explorer](#)

example:

```
https://api.dropboxapi.com/2/users/features/get_values
```

for a given account, verify the available features before testing.

next:

1. "What are all the ways I can access this account?"
2. "What are all the ways I can block myself from accessing this account?"
3. "What types of access can I give to others?"
4. "How can I revoke access given to others?"
5. "How can I see who accessed this account?"

account-access/acc

organize/move

Tests should expose flaws, and also validate successful compliance outcomes to inform risk-based decisions based on the totality of evidence.

Provide all stakeholders access to the tools and methodology used to reach conclusions.

NIST Privacy Framework Methodology

FUNCTION

IDENTIFY-P (ID-P)

Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

CATEGORY

Inventory and Mapping (ID.IM-P):
Data processing by systems, products, or services is understood and informs the management of privacy risk.

SUBCATEGORY

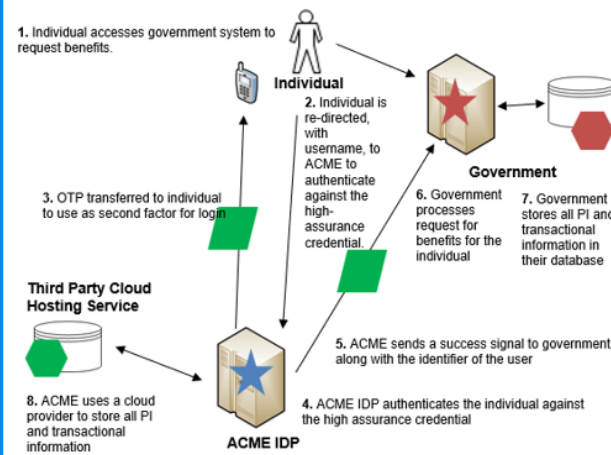
ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems /products /services, including components; roles of the component owners/operators; and interactions of individuals or third parties.

Data Processing Action:

Identify all components involved in processing personal data when verifying a consumer's identity.

Question: "How do we map all these components, and verify that our maps are accurate?"

Use of credential to access benefits



Use **Worksheet 2: Supporting Data Map from the NIST PRAM.**

The PRAM is a Privacy Risk Assessment Model which uses the NIST Privacy Framework to inform the management of privacy risk.

EVERYONE'S GUIDE TO THE CCPA

Authored by Craig Erickson, a California Consumer

This guide is only a small preview of a tool, formatted as an Excel workbook, which will be published on the NIST website as a contribution to the NIST Privacy Framework Resources and maintained by active contributors in the NIST repository on Github here: <https://github.com/usnistgov/PrivacyFrmwkResources/tree/master/resources>.

For additional information, online demonstrations, or free preview access to the entire tool, including the CCPA Test Suites and examples for using Privacy Framework Resources, please contact:

Craig Erickson, CIPT

craig-erickson@privacyportfolio.com

August 2023