

May 9, 2018

`require('lx')`

Performance and scaling a SaaS web application

Anže Pečar
@smotko

About me

Reciprocity

Bootstrapped

From 4 to 20 engineers

From 1 to 100 customers

ZenGRC

Compliance & Risk Management

ZenGRC

New

DASHBOARD

PROGRAMS

AUDITS

ISSUES

VENDORS

INFOSEC RISKS

SYSTEM OF RECORD

TO-DO LIST

TOOLS

SETTINGS

User profile

Privacy Policy

Copyright © v2.17

All Programs

EU GDPR Program

Program Info

Controls (4)

Objectives (200)

People (1)

Sections (46)

Standards (12)

Add...

Filter

Reset

OBJECTIVE TITLE	OWNER	STATE	
▶ Article 5.1	Dave	Draft	<div>+</div> <div>View</div>
▶ Article 5.2	Dave	Draft	<div>+</div> <div>View</div>
▶ Article 6.1	Dave	Draft	<div>+</div> <div>View</div>
▼ Article 6.2	Dave	Draft	<div>+</div> <div>View</div>

TITLE

Article 6.2 DRAFT

OBJECT REVIEW

Submit For Review

DESCRIPTION

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX

Spreadsheets

Challenges

High developer churn

Feature volatility

42k lines of JS to 82k

Bad Performance

Know your domain

Know your users

Lab *vs.* field data

10s load times

[← All Programs](#) **PCI-DSS 3.2 Security Program (Reference Program)**

 1
 281
 281
 1
 2
 13
 1
 9
 Add...

Program Info

TITLE

PCI-DSS 3.2 Security Program (Reference Program) FINAL

FINAL

OBJECT REVIEW

✓ REVIEWED ON 03/24/2018 10:34:43 PM
AND APPROVED BY РОМАН КОСМИНА ЙЦНГШШ

DESCRIPTION

The PCI Data Security Standard specifies 12 requirements for compliance, organized into six logically related groups called "control objectives". Each version of PCI DSS has divided these 12 requirements into a number of sub-requirements differently, but the 12 high level requirements have not changed since the inception of the standard.

To comply with the PCI-DSS security standards the following high level tasks must be completed. Sub-tasks and procedures will be documented within the tool.

- Identify and Create company the PCI-DSS Policy and Procedures (PnP)
- Identify and Create the necessary company system / security processes
- Answer the Self Assessment Questionnaire (SAQ)
- Perform gap analysis of the SAQ and PCI-DSS Requirements
- Design and Configure Systems to meet PnP requirements
- Design or Re-mediate any discrepancies of the SAQ and PnP
- Perform a Risk Assessment (Annually)
- Perform Periodic Tasks as Required
- Procure an ASV Vendor

NOTES

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

MANAGER

nada@reciprocitylabs.com

PRIMARY CONTACT

nada@reciprocitylabs.com

SECONDARY CONTACT

None

PROGRAM URL

<https://www.pcisecuritystandards.org/>

REFERENCE URL

None

► **Show Advanced**

Text CA1

Rich text ca2

None

None

Created at 06/26/2017 12:11:52 PM WEST Modified by Роман Космина ЙЦНГШЩ on 03/24/2018 10:34:43 PM WET

CLASSIC ☒ BETA ?



Reading from local storage

Using ORMs

**CPU time for things that aren't
even displayed**

← Programs

Actions

PCI-DSS 3.2 Security Program (Reference Program)

Description

The PCI Data Security Standard specifies 12 requirements for compliance, organized into six logically related groups called "control objectives". Each version of PCI DSS has divided these 12 requirements into a number of sub-requirements differently, but the 12 high level requirements have not changed since the inception of the standard.

To comply with the PCI-DSS security standards the following high level tasks must be completed. Sub-tasks and procedures will be documented within the tool.

- Identify and Create company the PCI-DSS Policy and Procedures (PnP)
- Identify and Create the necessary company system / security processes
- Answer the Self Assessment Questionnaire (SAQ)
- Perform gap analysis of the SAQ and PCI-DSS Requirements
- Design and Configure Systems to meet PnP requirements
- Design or Re-mediate any discrepancies of the SAQ and PnP
- Perform a Risk Assessment (Annually)
- Perform Periodic Tasks as Required
- Procure an ASV Vendor

Manager*

State*

Primary Contact

nada@reciprocitylabs.com

Final

nada@reciprocitylabs.com

DETAILS

MAPPED OBJECTS

HISTORY

SURVEYS

Assessments (1)

Controls (281)

Objectives (281)

People (1)

Projects (2)

Sections (13)

Map/Unmap

Export CSV

⚙

Standards (1)

Systems (9)

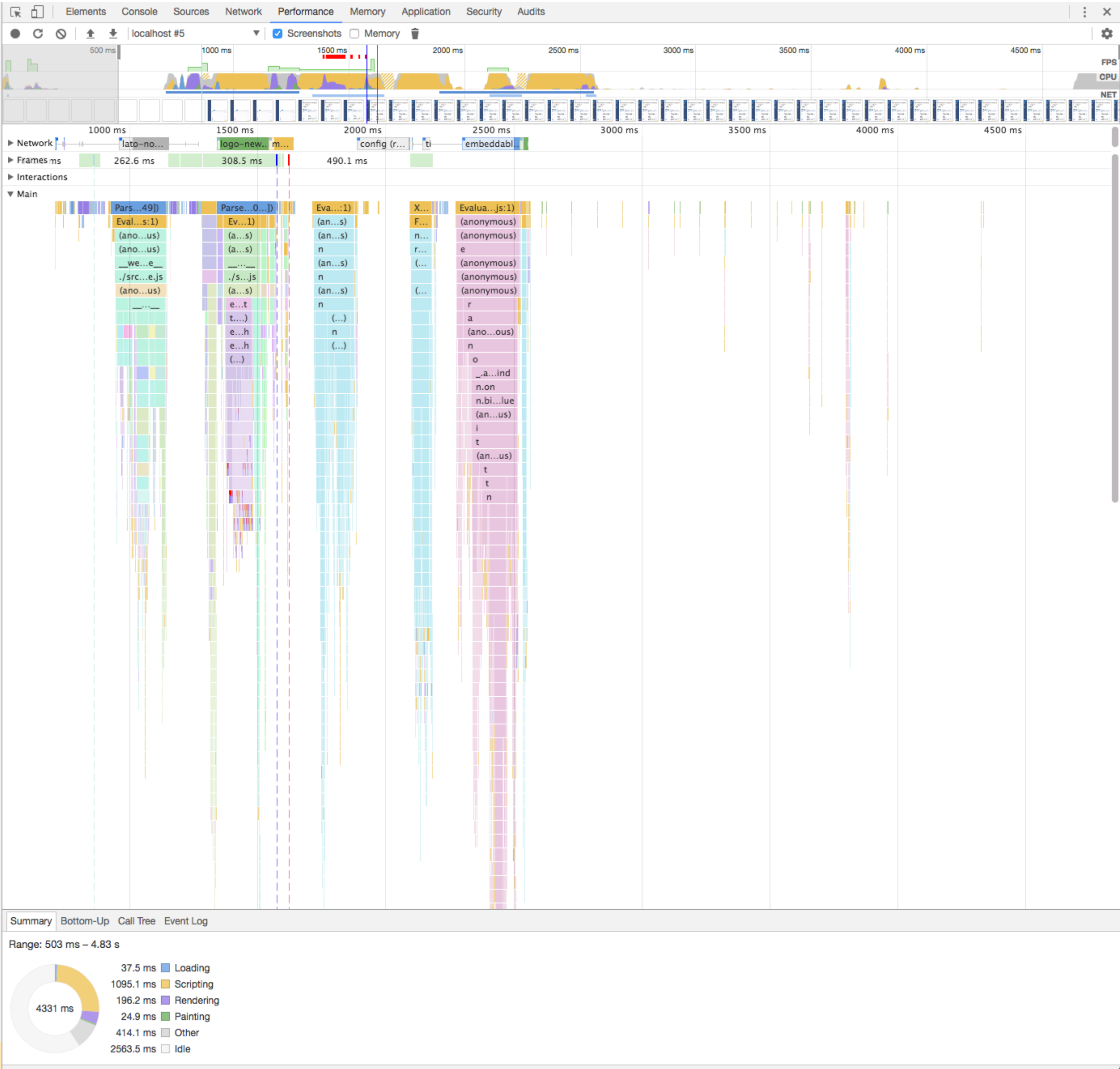
Add +

<input type="checkbox"/>	Title*	Description	Actions
<input type="checkbox"/>	▶ C-PCI-001	300 controls mapped to program - ADMIN is owner - System mapped to control "Notes" filed was not imported so it should... More	Send a survey
<input type="checkbox"/>	▶ C-PCI-002	300 controls mapped to program - ADMIN is owner - System mapped to control "Notes" filed was not imported so it should... More	Send a survey
<input type="checkbox"/>	▶ C-PCI-003	300 controls mapped to program - ADMIN is owner - System mapped to control "Notes" filed was not imported so it should... More	Send a survey
<input type="checkbox"/>	▶ C-PCI-004	300 controls mapped to program - READER is owner System mapped to control	Send a survey
<input type="checkbox"/>	▶ C-PCI-005	300 controls mapped to program - READER is owner System mapped to control	Send a survey
<input type="checkbox"/>	▶ C-PCI-006	300 controls mapped to program - READER is owner System mapped to control	Send a survey
<input type="checkbox"/>	▶ C-PCI-007	300 controls mapped to program - READER is owner System mapped to control	Send a survey
<input type="checkbox"/>	▶ C-PCI-008	300 controls mapped to program - READER is owner System mapped to control	Send a survey
<input type="checkbox"/>	▶ C-PCI-009	300 controls mapped to program - READER is owner System mapped to control	Send a survey
<input type="checkbox"/>	▶ C-PCI-010	300 controls mapped to program - READER is owner	Send a survey

CLASSIC

☒ BETA

?



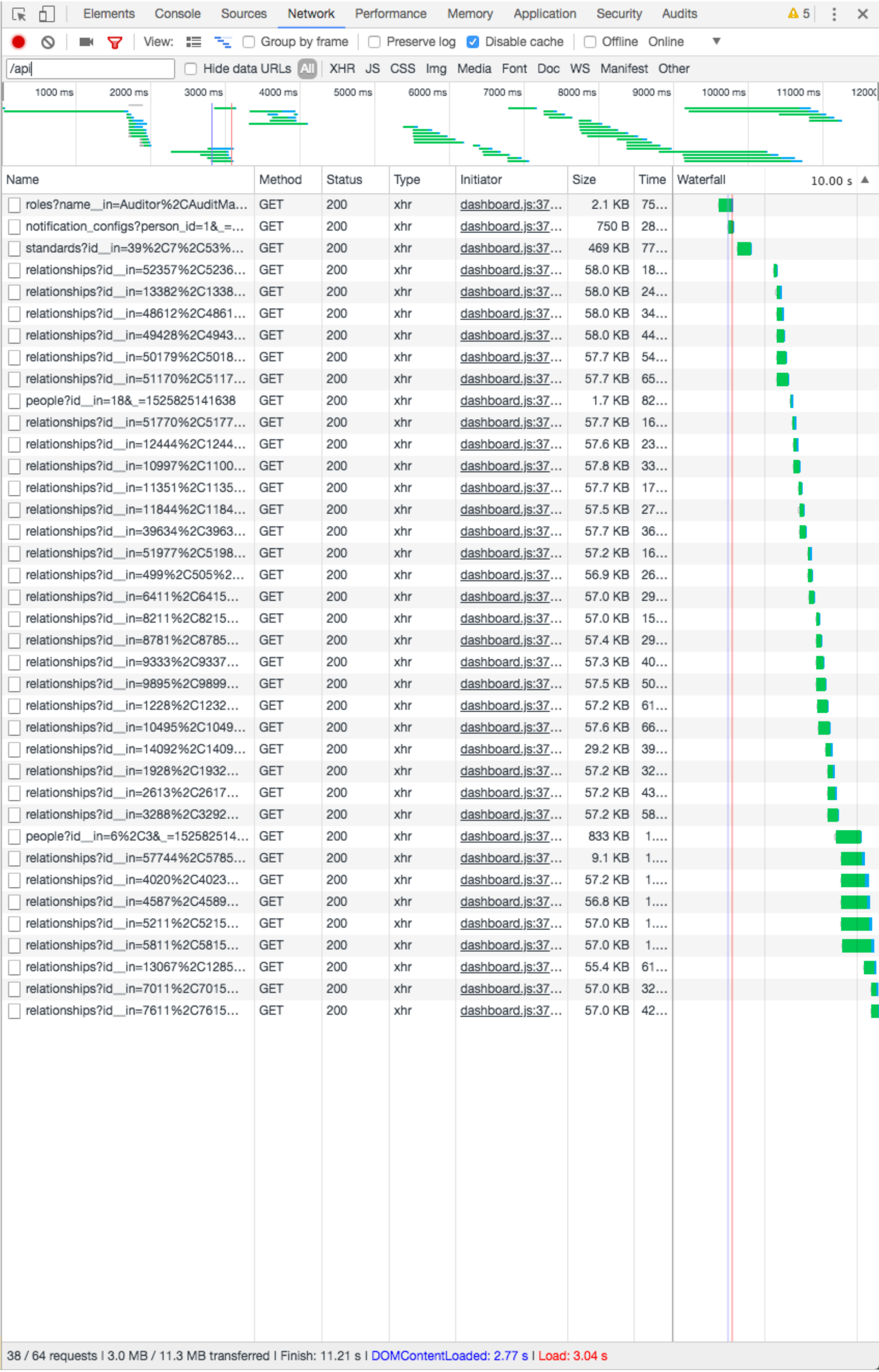
Network requests

Standards

Filter

Reset

STANDARD TITLE	OWNER	STATE		
▶ CJIS Standard	nada@reciprocitylab...	Draft	13	View
▶ COSO Principles	nada@reciprocitylab...	Draft	5	View
▶ COSO Principles БДФЙ ĆŽ	nada@reciprocitylab...	Draft	5	View
▶ DETECT (DE)	nada@reciprocitylab...	Draft	3	View
▶ FedRAMP LOW/MOD Standard	nada@reciprocitylab...	Draft	17	View
▶ HIPAA Breach Notification Rule	nada@reciprocitylab...	Draft	7	View
▶ HIPAA Privacy Rule	nada@reciprocitylab...	Draft	15	View
▶ HIPAA Security Rule	nada@reciprocitylab...	Draft	5	View
▶ HiTrust Standard	Dávid Máté Auguszt...	Draft	14	View
▶ IDENTIFY (ID)	nada@reciprocitylab...	Draft	5	View
▶ ISO/IEC 27001:2013 Standard - ISMS	nada@reciprocitylab...	Draft	9	View
▶ NIST 800-53 Standard	nada@reciprocitylab...	Draft	18	View
▶ PCI-DSS 3.2 Requirements	nada@reciprocitylab...	Draft	13	View
▶ PROTECT (PR)	nada@reciprocitylab...	Draft	6	View
▶ RECOVER (RC)	nada@reciprocitylab...	Draft	3	View
▶ RESPOND (RS)	nada@reciprocitylab...	Draft	5	View
▶ Standard mp001 2.13	Юзер Едітор	Draft	1	View
▶ Standard mp001 2.15	Роман Космина ЙЦ...	Draft	0	View
▶ Standard mp002 2.15	Роман Космина ЙЦ...	Draft	2	View
▶ Trust Services Principles and Criteria	nada@reciprocitylab...	Draft	5	View
▶ stand1	Роман Космина ЙЦ...	Draft	0	View
▶ pavin	Роман Космина ЙЦ...	Draft	0	View



**Only fetch what's actually
needed**

ZenGRC

New

DASHBOARD

PROGRAMS

AUDITS

ISSUES

VENDORS

INFOSEC RISKS BETA

SYSTEM OF RECORD

TO-DO LIST

TOOLS

SETTINGS

SUPPORT

nada@reciprocit...

Privacy Policy

Copyright © v2.19-DEV

Sections

Title*

800-53_AC Access Control

800-53_AT Awareness and Training

800-53_AU Audit and Accountability

800-53_CA Security Assessment and Authorization

800-53_CM Configuration Management

800-53_CP Contingency Planning

800-53_IA Identification And Authentication

800-53_IR Incident Response

800-53_MA Maintenance

800-53_MP Media Protection

800-53_PE Physical and Environmental Protection

800-53_PL Planning

800-53_PS Personnel Security

800-53_RA Risk Assessment

800-53_SA System and Services Acquisition

800-53_SC System and Communications Protection

800-53_SI System and Information Integrity

800-53_PM Information Security Program Plan

PCI Requirement 1 - Firewall Configuration

PCI Requirement 2 - System Passwords and Configuration

Text of Section

The Access Control (AC) control family is based around the policies and procedures over the following: Access Control...
[More](#)

The Awareness and Training (AT) control family is based around the policies and procedures over the following: ...
[More](#)

The Audit and Accountability (AU) control family is based around the policies and procedures over the following:
[More](#)

The Security Assessment and Authorization (CA) control family specifies organization-defined parameters that are...
[More](#)

The Configuration Management (CM) control family is a collection of activities focused on establishing and...
[More](#)

Contingency Planning

Identification And Authentication

Incident Response

Maintenance

Media Protection

Physical and Environmental Protection

Planning

Personnel Security

Risk Assessment

System and Services Acquisition

System and Communications Protection

System and Information Integrity

Information Security Program Plan

Install and maintain a firewall configuration to protect cardholder data

Do not use vendor-supplied defaults for system passwords and other security parameters

Owner*

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

nada@reciprocitylabs.com

State*

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Draft

Rows per page: 20

<

1

2

3

...

7

8

>

CLASSIC

BETA

?

Elements

Console

Sources

Network

Performance

Memory

Application

Security

Audits

View:

Group by frame

Preserve log

Disable cache

Offline

Online

/sor

Hide data URLs

All

XHR

JS

CSS

Img

Media

Font

Doc

WS

Manifest

Other

200 ms

400 ms

600 ms

800 ms

1000 ms

1200 ms

1400 ms

1600 ms

1800 ms

2000 ms

2200 ms

2400 ms

Name

Method

Status

Type

Initiator

Size

Time

Waterfall

2.00 s

▲

Section

GET

302

text/html

Other

639 B

37...

Section?fields=title%2Cdescription%...

GET

200

document

:8080/sor/listing...

117 KB

27...

sor_listing.css?v=9ab4951

GET

200

stylesheet

Section?fields=t...

5.5 KB

73...

sor_listing.js?v=9ab4951

GET

200

script

Section?fields=t...

91.1 KB

52...

4 / 27 requests | 214 KB / 6.7 MB transferred | Finish: 2.21 s | DOMContentLoaded: 1.21 s | Load: 1.34 s

The list view

New

DASHBOARD

PROGRAMS

AUDITS

ISSUES

VENDORS

SYSTEM OF RECORD

TO-DO LIST

TOOLS

SETTINGS

SUPPORT

nada@reciprocity... ^

Controls

Filter

✓

Q

Reset



CONTROL TITLE	OWNER	STATE	
▼ 2.13 C EFFECTIVE control - No objective	Object Reader	Draft	View
MAPPED OBJECTS			
2.13 Request Admin 001 - Open			View
2.13 Request Editor 003			View
2.13 Request Reader 007			View
2.13 Request Creator 009 - WITHOUT verifier - Overdue			View
🔓 2.13-1 A2 EFFECTIVE-Control Assessment			View
🔓 2.13-1 A3 EFFECTIVE-Control Assessment			View
👁 Audit Draft 2.13			View
👁 Audit Internal 2.13			View
👁 Piki			View
🚨 I Assigned Issue 2.13			View
👁 Audit Internal 2.13-1			View
📁 2.18 rc4			View
👤 proc1			View
👁 NIST 800-53 Internal Audit - 1000 controls/assessment/requests			View
📁 111112			View

TITLE

2.13-1 A2 EFFECTIVE-Control Assessment

OPEN

DESCRIPTION

None

MAPPED OBJECTS

▶ 2.13 C EFFECTIVE control - No objective

View

▶ Audit Internal 2.13-1

View

▶ 2.13 P Audit Dashboard

View

ROLES

C

CREATOR(S) • Роман Космина ЙЦНГШЩ

A

ASSESSOR(S) • Object Reader

V

VERIFIER(S) No verifiers

DATES

REPEATS

Never

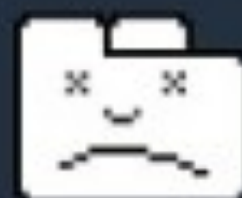
STARTS ON

08/10/2017

Map Objects

EVIDENCE

Add evidence URL



Aw, Snap!

Something went wrong while displaying this webpage. To continue, reload or go to another page.

If you're seeing this frequently, try [these suggestions](#).

Lazy loading

All objects

5

3288

37

4

4

2335

4

19

45

22

2449

4

29

6

3

32

3

2

3455

149

22

58

7

3

209

8

15

SECTION TITLE	OWNER	STATE				
▶ HiTrust 03.0 - Risk Management	Dávid Máté Augusztinovicz	Draft	7	1	4	View
▶ HiTrust 04.0 - Security Policy	Dávid Máté Augusztinovicz	Draft	5	1	2	View
▶ HiTrust 05.0 - Organization of Information Security	Dávid Máté Augusztinovicz	Draft	15	2	11	View
▶ HiTrust 06.0 - Compliance	Dávid Máté Augusztinovicz	Draft	15	3	10	View
▶ HiTrust 07.0 - Asset Management	Dávid Máté Augusztinovicz	Draft	9	2	5	View
▶ HiTrust 08.0 - Physical and Environmental Security	Dávid Máté Augusztinovicz	Draft	17	2	13	View
▶ HiTrust 09.0 - Communications and Operations Management	Dávid Máté Augusztinovicz	Draft	44	10	32	View
▶ HiTrust 10.0 - Information Systems Acquisition, Development...	Dávid Máté Augusztinovicz	Draft	21	6	13	View
▶ HiTrust 11.0 - Information Security Incident Management	Dávid Máté Augusztinovicz	Draft	9	2	5	View
▶ HiTrust 12.0 - Business Continuity Management	Dávid Máté Augusztinovicz	Draft	8	1	5	View
▶ HiTrust 13.0 - Privacy Practices	Dávid Máté Augusztinovicz	Draft	19	3	14	View

New

All objects














🔧 5 🔄 3288 👁 37 📄 4 📁 4 🎥 2335 💾 4 🏢 19 ⚠ 45 🛒 22 🎯 2449 👥 4 📄 29 📊 6 📁 3 📁 32 📦 3 📄 2 📄 3455 🗣 149 📄 22 ⚙ 58 📁 7 📁 3 ⚡ 209 📅 8 📅 15

Filter

✔

Reset

?

OBJECTIVE TITLE	OWNER	STATE	   	
▶ 164.308(a)(1)(i) Security Mgmt Process	nada@reciprocitylabs.com	In Scope		View
▶ 164.308(a)(1)(ii)(A) Risk Analysis (R)	nada@reciprocitylabs.com	In Scope		View
▶ 164.308(a)(1)(ii)(B) Risk Mgmt (R)	nada@reciprocitylabs.com	In Scope		View
▶ 164.308(a)(1)(ii)(C) Sanction Policy (R)	nada@reciprocitylabs.com	In Scope		View
▶ 164.308(a)(1)(ii)(D) Information System Activity Review (R)	nada@reciprocitylabs.com	In Scope		View
▶ 164.308(a)(2) Assigned Security Responsibility	nada@reciprocitylabs.com	In Scope		View
▶ 164.308(a)(3)(i) Workforce Security	nada@reciprocitylabs.com	In Scope		View
▶ 164.308(a)(3)(ii)(A) Authorization and/ or Supervision (A)	nada@reciprocitylabs.com	In Scope		View
▶ 164.308(a)(3)(ii)(B) Workforce Clearance Procedures (A)	nada@reciprocitylabs.com	In Scope		View
164.308(a)(3)(ii)(C) Termination Procedures (A)				
164.308(a)(4)(i) Information Access Management				

DASHBOARD >

PROGRAMS

AUDITS

ISSUES

VENDORS

SYSTEM OF RECORD >

TO-DO LIST

TOOLS >

SETTINGS >

SUPPORT

nada@reciprocity... ^

Privacy Policy

Rewrite in react

Pagination

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1																										
2																										
3																										
4																										
5																										
6																										
7																										
8																										
9																										
10																										
11																										
12																										
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																										

New in Sheets!

Macro recorder, row & column grouping, printing improvements, checkboxes, and more!

[LEARN MORE](#) [GOT IT](#)

New

DASHBOARD >

PROGRAMS

AUDITS

ISSUES

VENDORS

INFOSEC RISKS BETA

SYSTEM OF RECORD >

TO-DO LIST

TOOLS >

SETTINGS >

SUPPORT

nada@reciprocit... ^

Objectives



Actions



<input type="checkbox"/>	Title*	Description More	Owner*	State*	Primary Contact	Actions
<input type="checkbox"/>	▶ 800-53_AC-2 (3) - Disable Inactive Accounts	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey
<input type="checkbox"/>	▶ 800-53_AC-2 (4) - Automated Audit Actions	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and... More	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey
<input type="checkbox"/>	▶ 800-53_AC-2 (5) - Inactivity Logout	The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or... More	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey
<input type="checkbox"/>	▶ 800-53_AC-2 (6) - Dynamic Privilege Management	The information system implements the following dynamic privilege management capabilities: [Assignment:... More	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey
<input type="checkbox"/>	▶ 800-53_AC-2 (7) - Role-Based Schemes	The organization: - Establishes and administers privileged user accounts in accordance with a role-based access scheme... More	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey
<input type="checkbox"/>	▶ 800-53_AC-2 (8) - Dynamic Account Creation	The information system creates [Assignment: organization-defined information system accounts] dynamically.	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey
<input type="checkbox"/>	▶ 800-53_AC-2 (9) - Restrictions On Use Of Shared / Group Accounts	The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for... More	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey
<input type="checkbox"/>	▶ 800-53_AC-2 (10) - Shared / Group Account Credential Termination	The information system terminates shared/group account credentials when members leave the group.	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey
<input type="checkbox"/>	▶ 800-53_AC-2 (11) - Usage Conditions	The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for... More	nada@reciprocitylabs.com	In Scope	nada@reciprocitylabs.com	Send a survey

Rows per page: 20 ▲

< 1 2 3 ... 122 123 >

Recap

Metrics & User behavior

CPU time only
for what the user sees

Load only what is needed

Try to avoid complete rewrites

QA

@smotko
anze@pecar.me