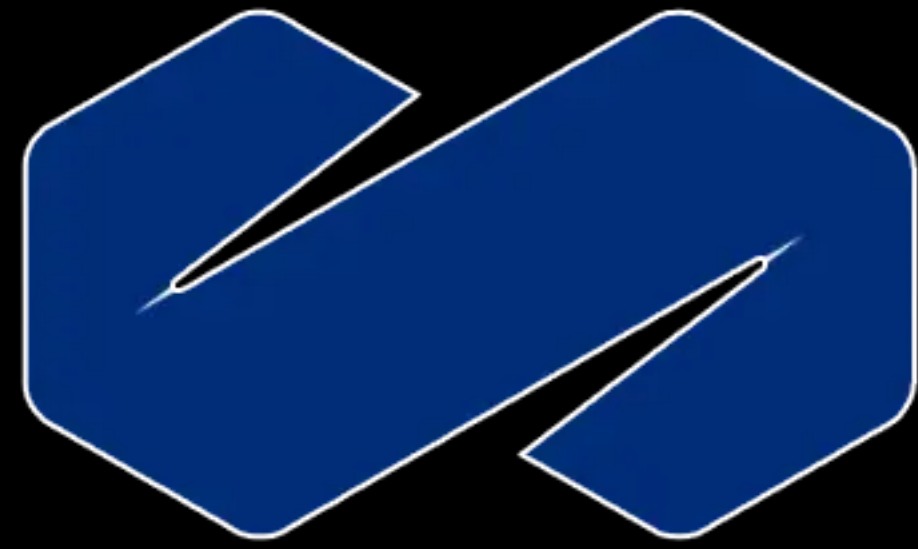




macOS Security Compliance



https://github.com/usnistgov/macos_security



MarshMcLennan

Using data to prioritize cybersecurity investments, automated hardening techniques were found, by a wide margin, to have the greatest ability of any control studied to decrease the likelihood of a successful cyberattack. Organizations with such techniques in place, which apply baseline security configurations to system components like servers and operating systems, are nearly six times less likely to have a cyber incident than those that do not.

Solving a Problem



- Yearly major release from Apple
- New hardware
- Out of date guidance

NLSST

NIST

DISA

NASA



Los Alamos
NATIONAL LABORATORY

NIST

DISA

NASA



Los Alamos
NATIONAL LABORATORY

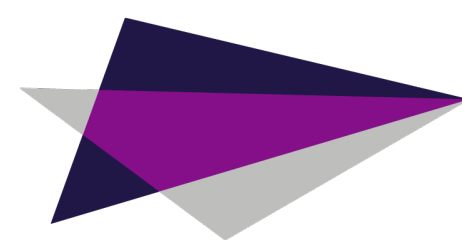


jamf



CIS

Center for Internet Security



leidos

ING, MI
PM

**If we work together,
we can accomplish anything.**

Apple Platform Certifications

Search this guide

[Table of Contents](#)

macOS Security Cor

The [macOS Security Compliance Project](#) is a programmatic approach to generating security profiles, output customized documentation, script profiles, and an audit checklist based on [Special Publication 800-219, Automated Security Compliance Project \(mSCP\)](#).

This is a joint project of federal operations and standards (NIST), National Institute of Standards and Technology (NIST), National Defense Information Systems Agency (NDISA). The project uses a set of tested and validated controls against any security guide supported by Apple. It can be used as a resource to easily create controls by leveraging a library of tested settings). The mSCP can produce output for management and security tools to achieve project support the following guidance:

Organization

National Institute of Standards and Technology (NIST) Special Publication (SP) [800-53](#), Recommended Security Controls for Federal Information Systems and Organizations, Revision 5


Apple Platform Certifications

Apple Platform Certifications

December 2022

Search this guide

[Table of Contents](#)




Operating systems

it-training.apple.com/tutorials/apt-deployment#developing-your-mac-compl


Deployment and Management Tutorials

- Introduction +
- MDM Planning +
- MDM Preparation +
- Device Enrollment +
- Device Management +
- Device Redeployment and Recycling +
- Exam Preparation +
- Mac Security Compliance** x
- Developing Your Mac Compliance Strategy



Mac Security Compliance

Develop a security strategy for Apple devices and use the macOS Security Compliance Project to meet compliance requirements for Mac computers.



Chapter 1 Developing Your Mac Compliance Strategy

Identify your organization's security strategy and plan for compliance. Learn how to use the macOS Security Compliance Project to generate baselines and guidance and to identify security gaps.

- Implementing a Security Strategy
- Preparing to Use the macOS Security Compliance Project
- Using the macOS Security Compliance Project
- Generating Baselines and Guidance
- Identifying Security Gaps

NIST SP 800-219

**NIST Special Publication
NIST SP 800-219**

Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)

Mark Trapnell
Eric Trapnell
Murugiah Souppaya
*Computer Security Division
Information Technology Laboratory*

Bob Gendler
*Customer Access and Support Division
Office of Information Systems Management*

Karen Scarfone
*Scarfone Cybersecurity
Clifton, VA*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-219>

June 2022



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology



macOS Security Compliance Project (mSCP)

- Ships alongside OS
- Tested Controls
- Fully Documented
- Scripts, Profiles, plists, and more
- Interagency tested, NIST approved
- Massive yearly effort reduction





Making Compliance Easy

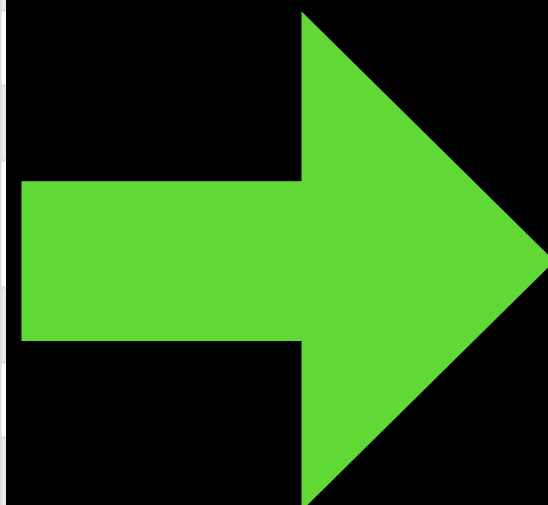
SP 800-53 Rev. 5.1 and SP 800-53B Latest Version

Controls Contain:

Moderate Security Baseline

Showing 177 controls

No.	Control Name	Low-Impact	Moderate-Impact	High-Impact
AC-1	POLICY AND PROCEDURES	AC-1	AC-1	AC-1
AC-2	ACCOUNT MANAGEMENT	AC-2	AC-2 (1) (2) (3) (4) (5) (13)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	ACCESS ENFORCEMENT	AC-3	AC-3	AC-3
AC-4	INFORMATION FLOW ENFORCEMENT		AC-4	AC-4 (4)
AC-5	SEPARATION OF DUTIES		AC-5	AC-5
AC-6	LEAST PRIVILEGE		AC-6 (1) (2) (5) (7) (9) (10)	AC-6 (1) (2) (3) (5) (7) (9) (10)
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	AC-7	AC-7	AC-7
AC-8	SYSTEM USE NOTIFICATION	AC-8	AC-8	AC-8
AC-11	DEVICE LOCK		AC-11 (1)	AC-11 (1)
AC-12	SESSION TERMINATION		AC-12	AC-12
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14	AC-14	AC-14
AC-17	REMOTE ACCESS	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	WIRELESS ACCESS	AC-18	AC-18 (1) (3)	AC-18 (1) (3) (4) (5)
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	AC-19	AC-19 (5)	AC-19 (5)
AC-20	USE OF EXTERNAL SYSTEMS	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	INFORMATION SHARING		AC-21	AC-21
AC-22	PUBLICLY ACCESSIBLE CONTENT	AC-22	AC-22	AC-22
AT-1	POLICY AND PROCEDURES	AT-1	AT-1	AT-1



```
id: os_airdrop_disable
title: "Disable AirDrop"
discussion:
  AirDrop _MUST_ be disabled to prevent file transfers to or from unauthorized devices.

  AirDrop allows users to share and receive files from other nearby Apple devices.
check: |
  /usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'allowAirDrop = 0'
result:
  integer: 1
fix: |
  This is implemented by a Configuration Profile.
references:
  cce:
    - CCE-90898-8
  cci:
    - CCI-000381
  800-53r5:
    - AC-3
    - AC-20
    - CM-7
    - CM-7(1)
  800-53r4:
    - CM-7
    - CM-7(1)
    - AC-3
    - AC-20
  srg:
    - N/A
  disa_stig:
    - N/A
  800-171r2:
    - 3.1.1
    - 3.1.2
    - 3.1.16
    - 3.1.20
    - 3.4.6
```


NIST Special Publication 800-53

Health Insurance Portability and Accountability Act

Financial Industry Regulatory Authority

Committee on National Security Systems Instruction

Center for Internet Security

International Organization for Standardization

Control Objectives for Information and Related Technologies

Payment Card Industry Data Security Standard

DISA Security Technical Implementation Guides

Health Information Technology for Economic and Clinical Health

Gramm-Leach-Bliley Act

Sarbanes-Oxley Act



NIST Special Publication 800-53

Health Insurance Portability and Accountability Act

Financial Industry Regulatory Authority

Committee on National Security Systems Instruction

Center for Internet Security

International Organization for Standardization

Control Objectives for Information and Related Technologies

Payment Card Industry Data Security Standard

DISA Security Technical Implementation Guides

Health Information Technology for Economic and Clinical Health

Gramm-Leach-Bliley Act

Sarbanes-Oxley Act



NIST Special Publication 800-53

Health Insurance Portability and Accountability Act

Financial Industry Regulatory Authority

Committee on National Security Systems Instruction

Center for Internet Security

International Organization for Standardization

Control Objectives for Information and Related Technologies

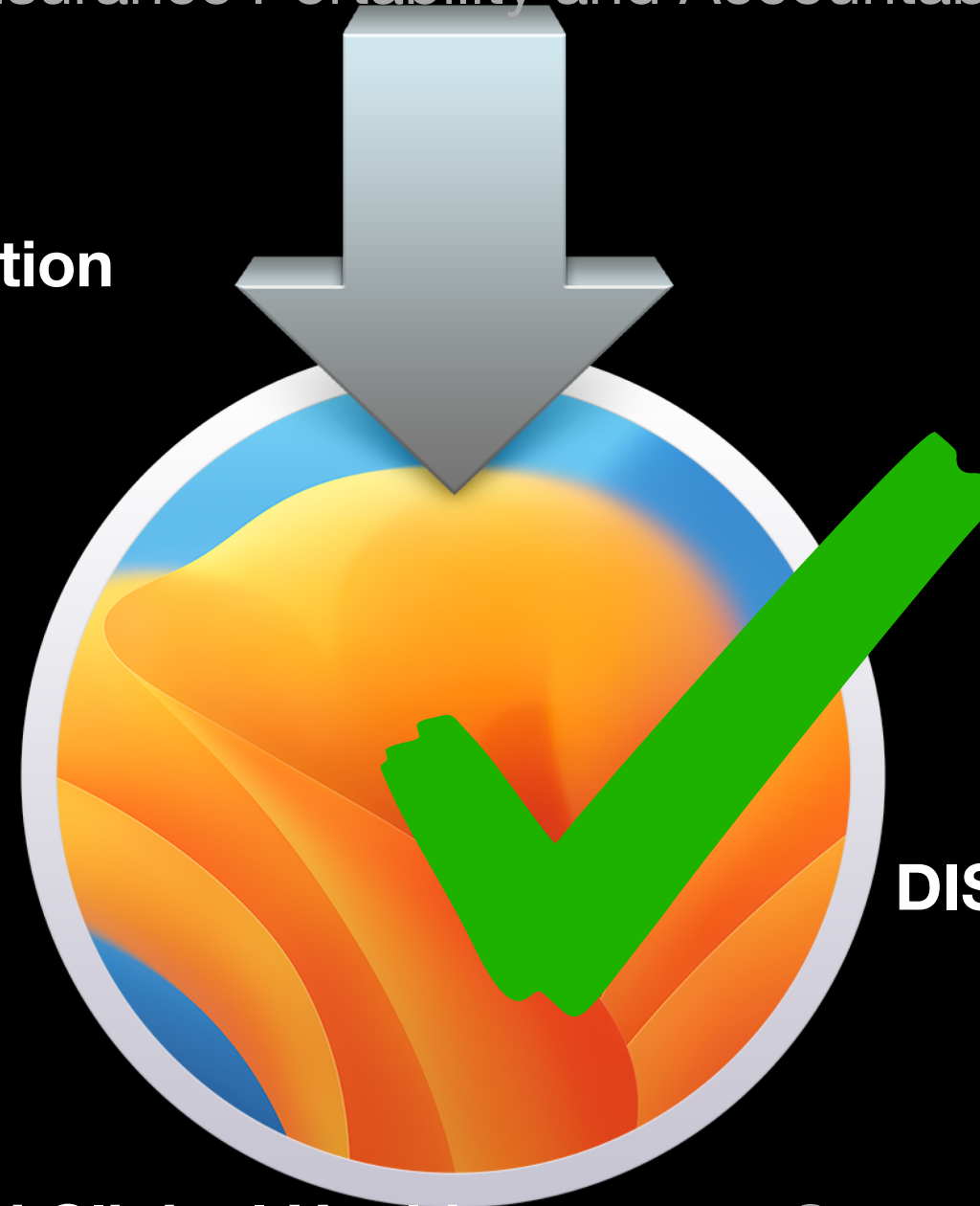
Payment Card Industry Data Security Standard

DISA Security Technical Implementation Guides

Health Information Technology for Economic and Clinical Health

Gramm-Leach-Bliley Act

Sarbanes-Oxley Act



NIST Special Publication 800-53

Health Insurance Portability and Accountability Act

Financial Industry Regulatory Authority

Committee on National Security Systems Instruction



Center for Internet Security

International Organization for Standardization

Control Objectives for Information and Related Technologies

Payment Card Industry Data Security Standard



DISA Security Technical Implementation Guides

Health Information Technology for Economic and Clinical Health

Gramm-Leach-Bliley Act

Sarbanes-Oxley Act

NIST Special Publication 800-53

Health Insurance Portability and Accountability Act

Financial Industry Regulatory Authority

Committee on National Security Systems Instruction

Center for Internet Security

International Organization for Standardization

Control Objectives for Information and Related Technologies

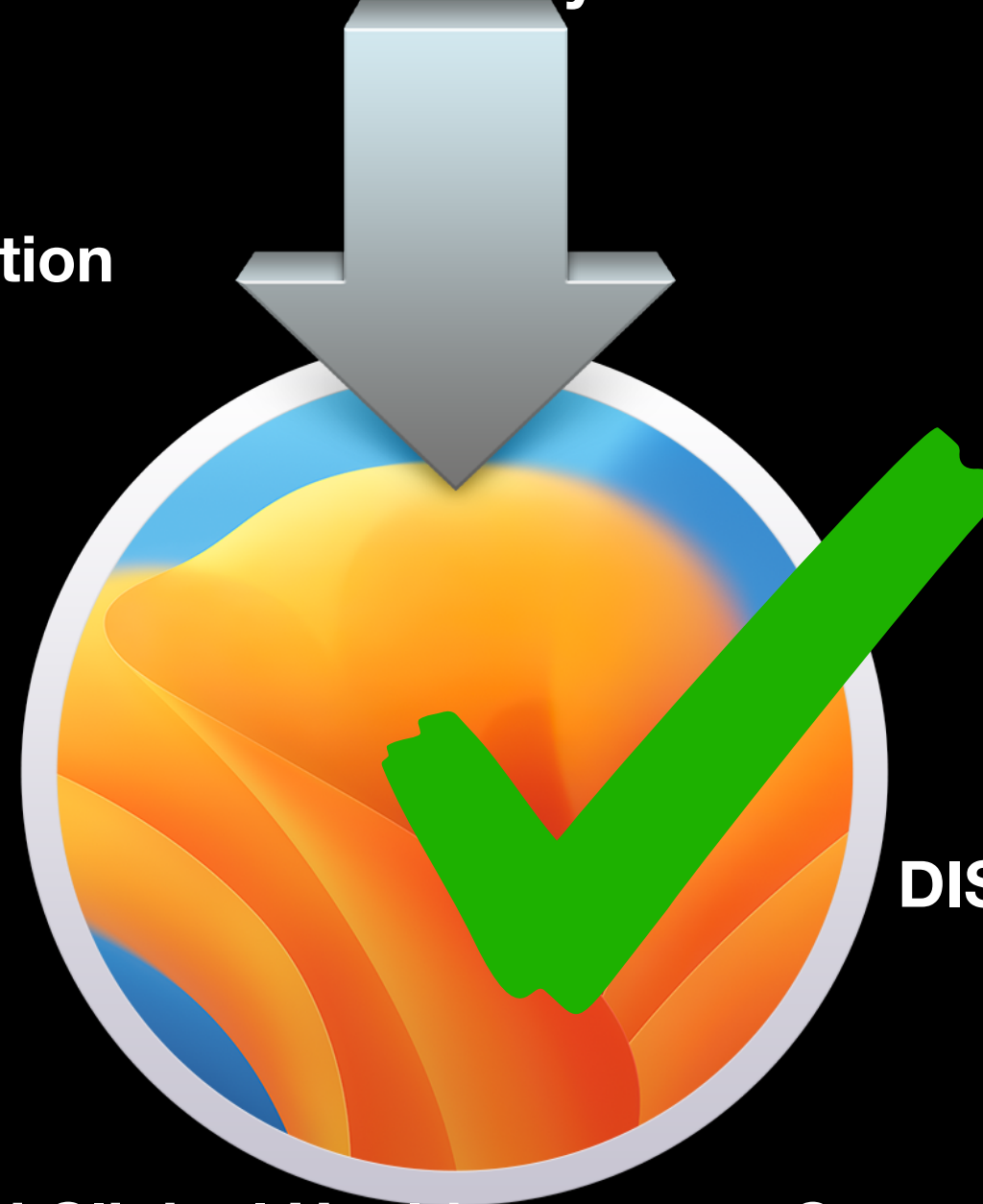
Payment Card Industry Data Security Standard

DISA Security Technical Implementation Guides

Health Information Technology for Economic and Clinical Health

Gramm-Leach-Bliley Act

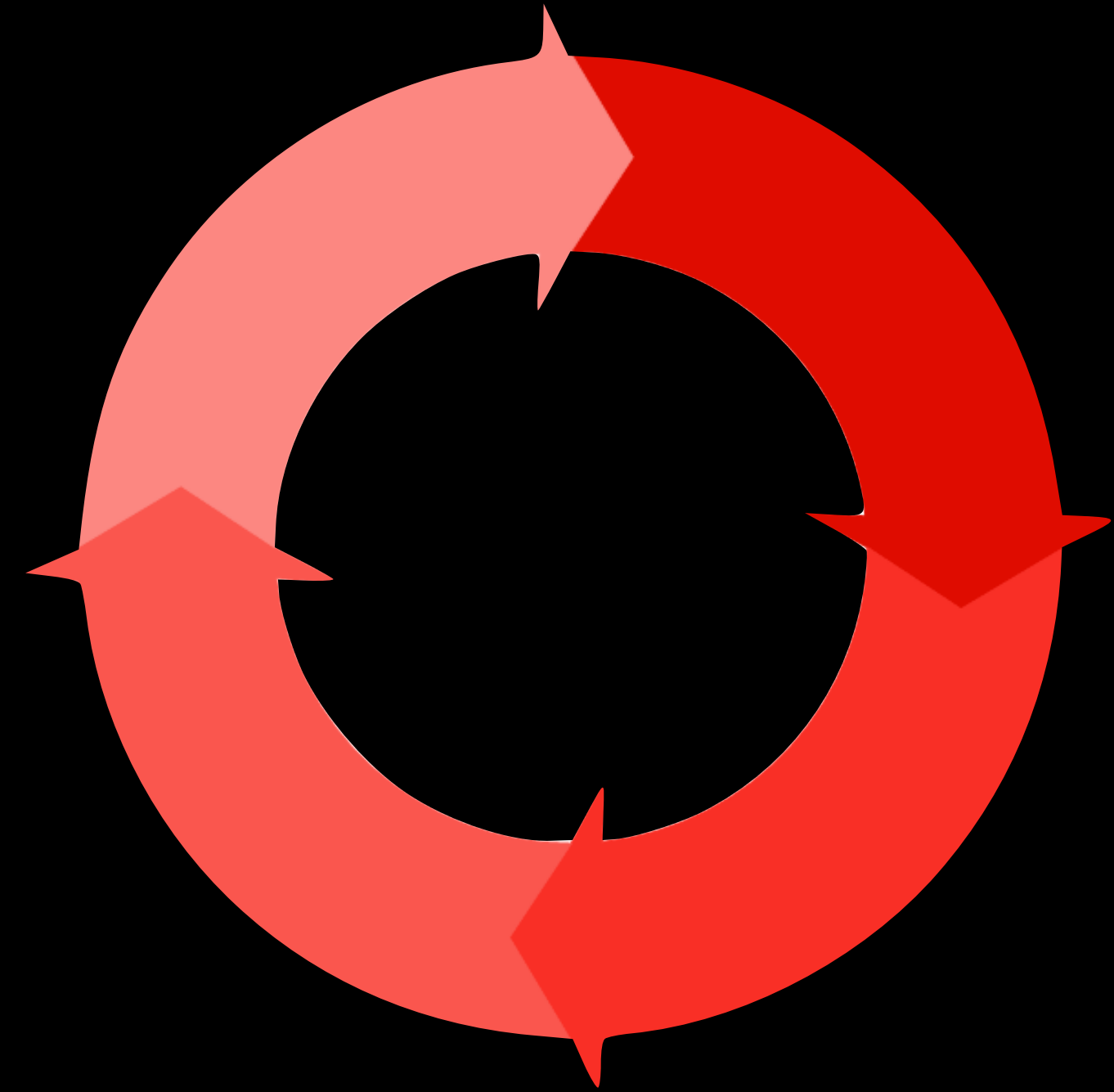
Sarbanes–Oxley Act







2020/06/09

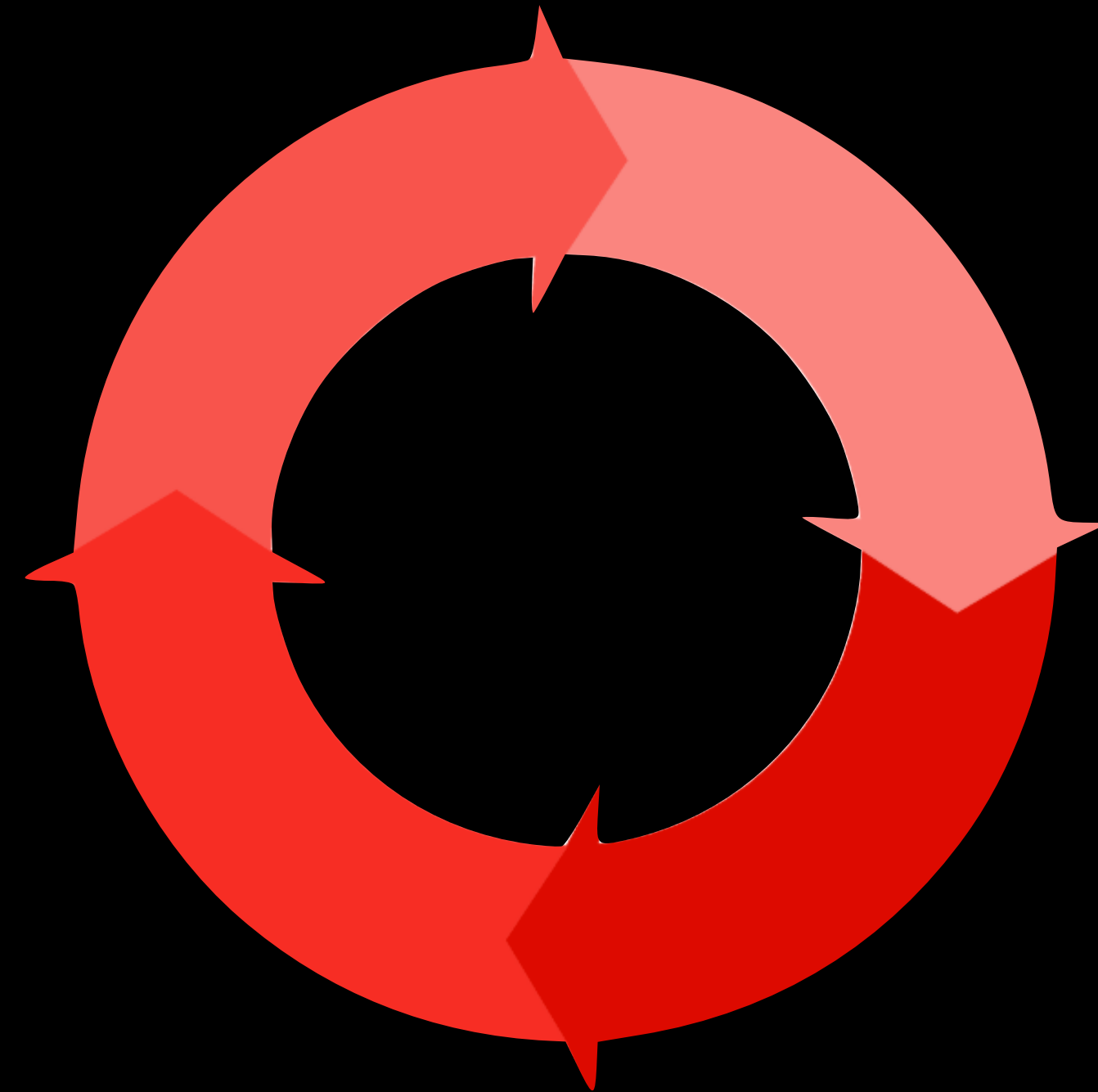




2020/06/09



2019/10/07

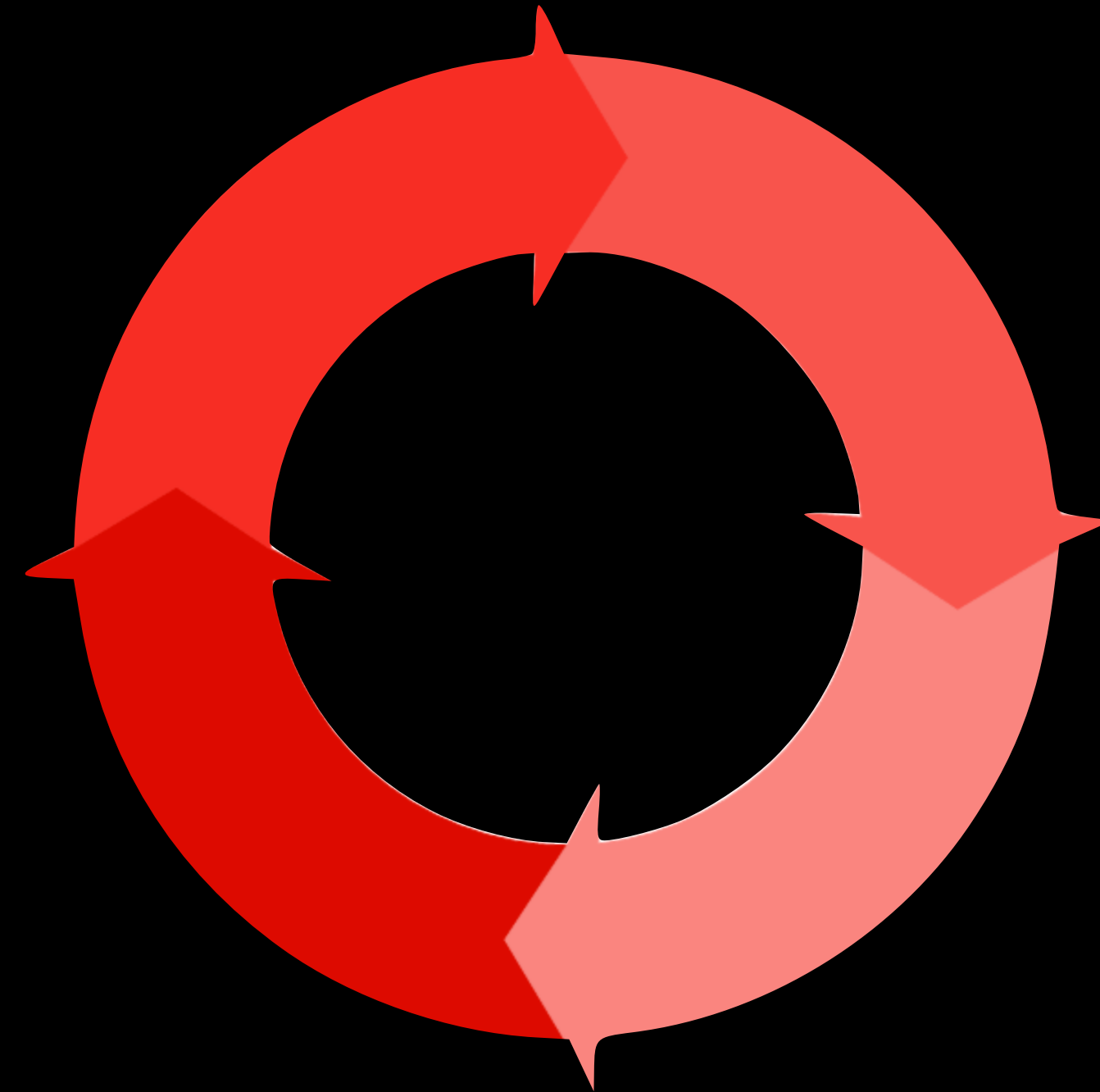




2020/06/09



2020/10/06





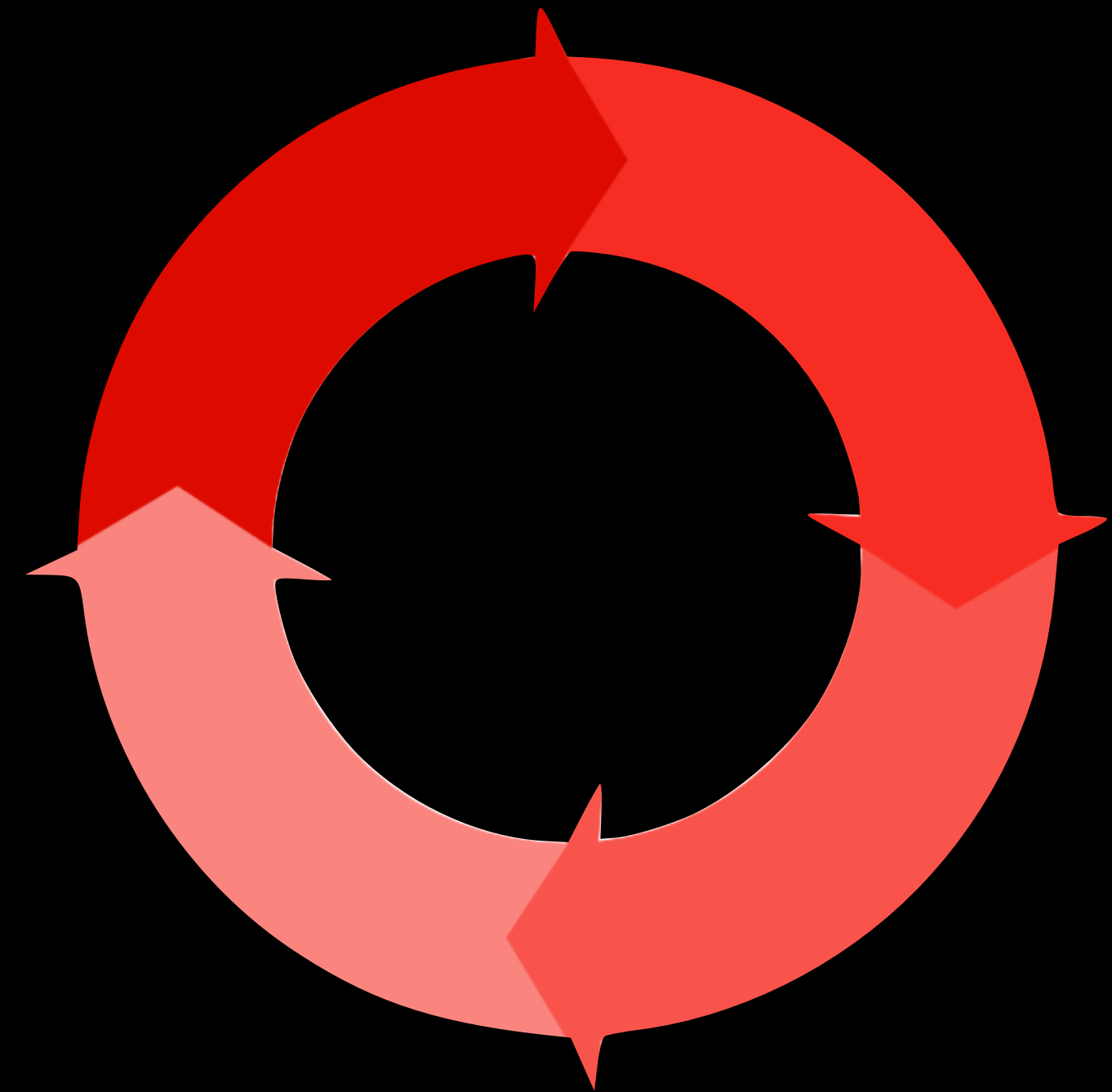
2020/06/09



2020/10/06



2020/11/12





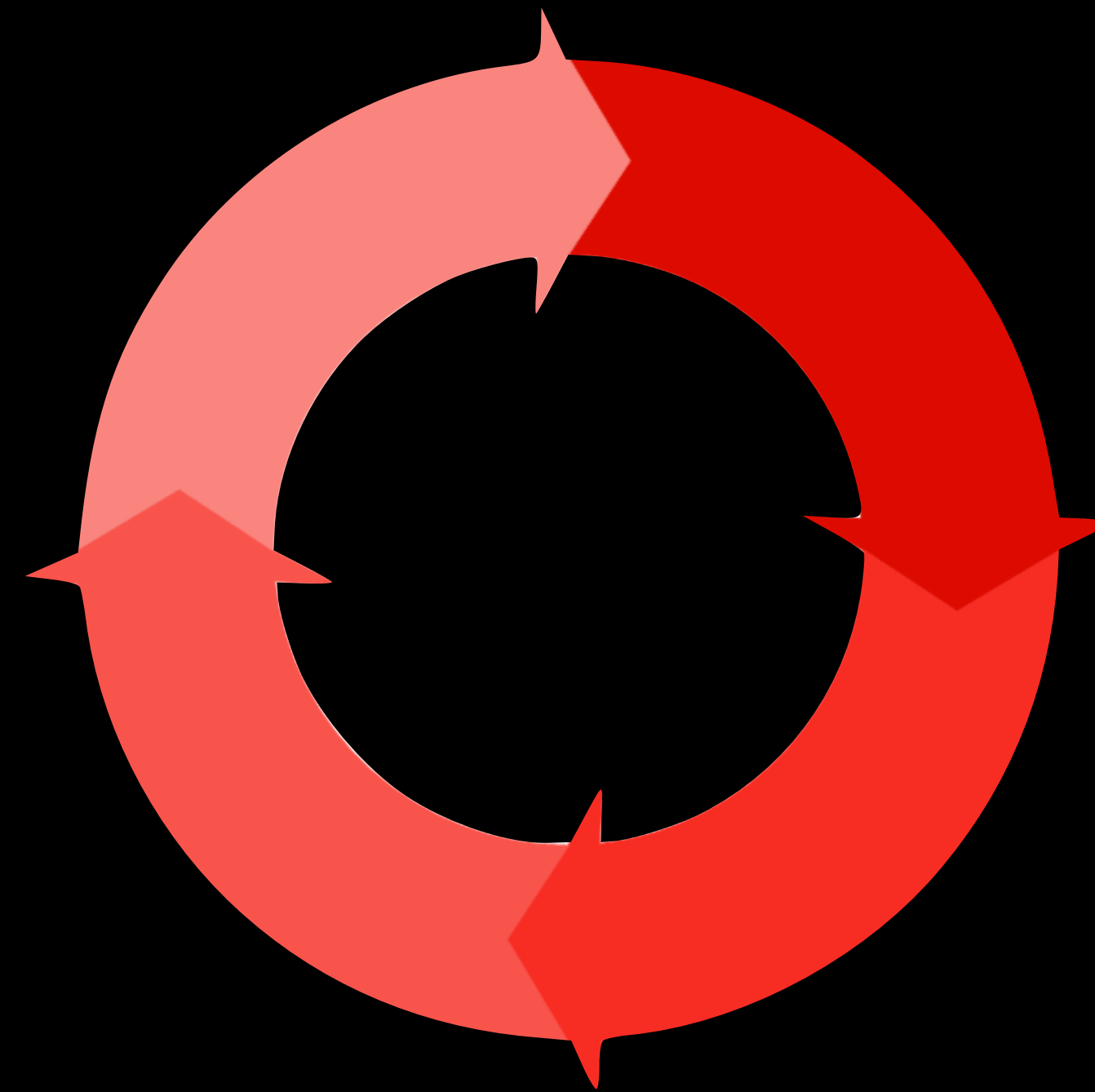
2020/06/09



2020/10/06



2020/11/10





2020/06/09



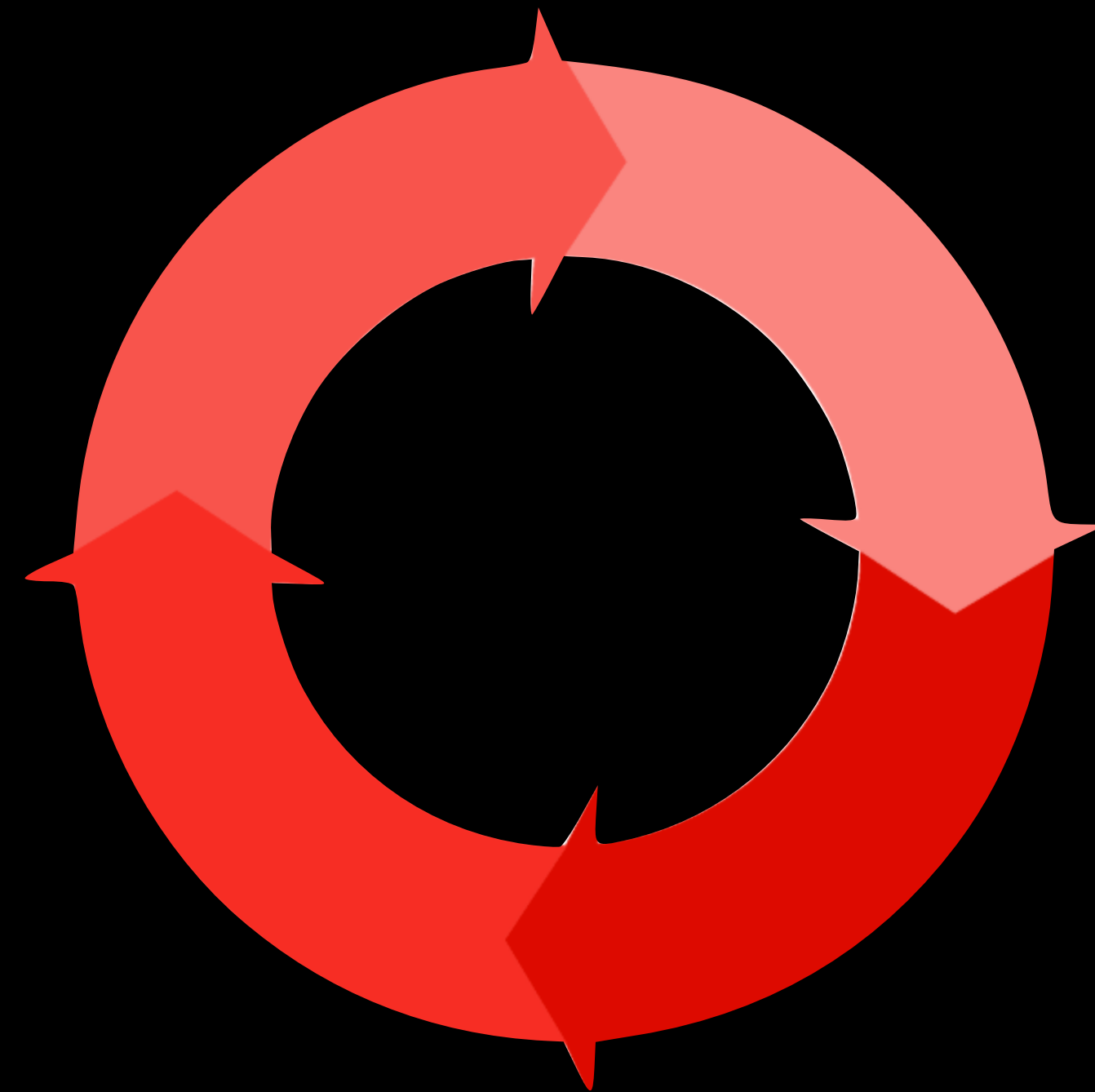
2020/10/06



2020/11/10



2021/10/25





2020/06/09



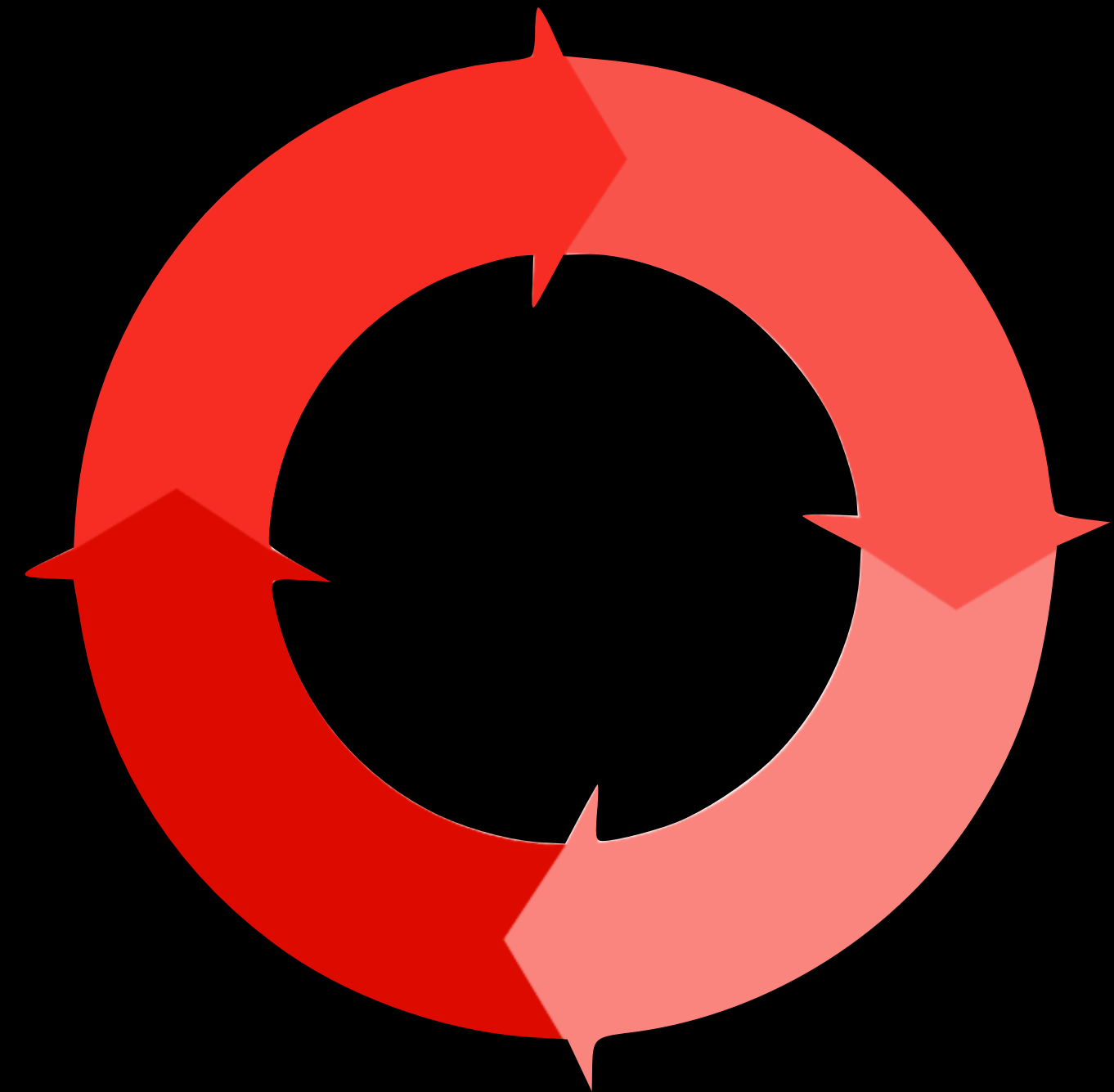
2020/10/06



2020/11/10



2021/10/20







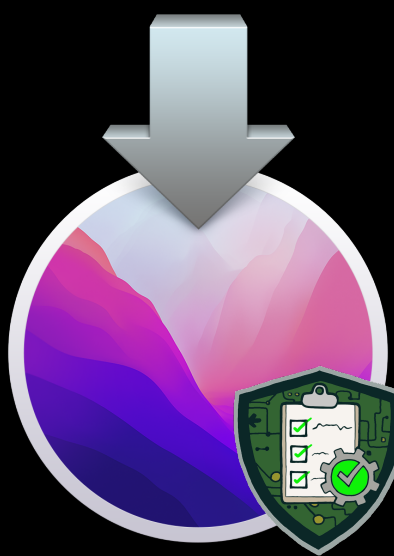
2020/06/09



2020/10/06



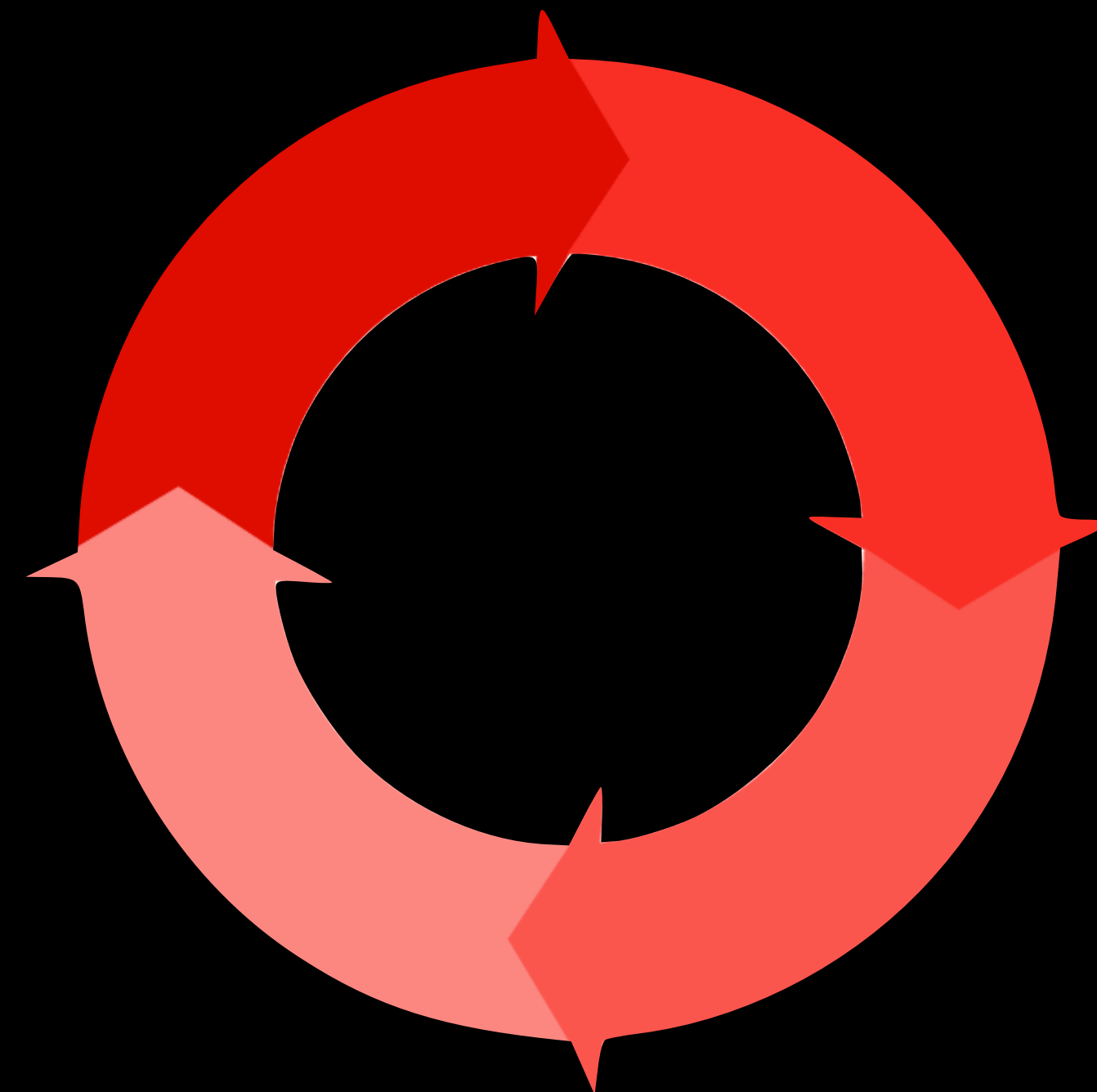
2020/11/10



2021/10/20



2022/10/24





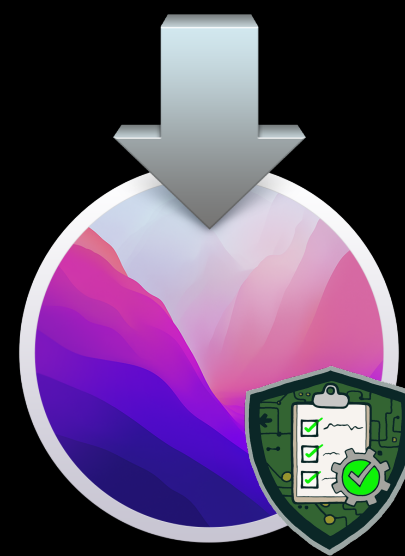
2020/06/09



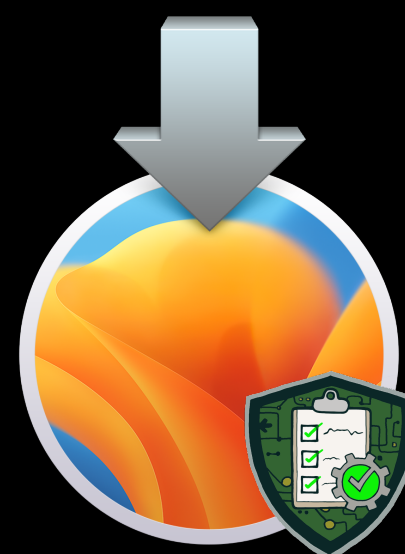
2020/10/06



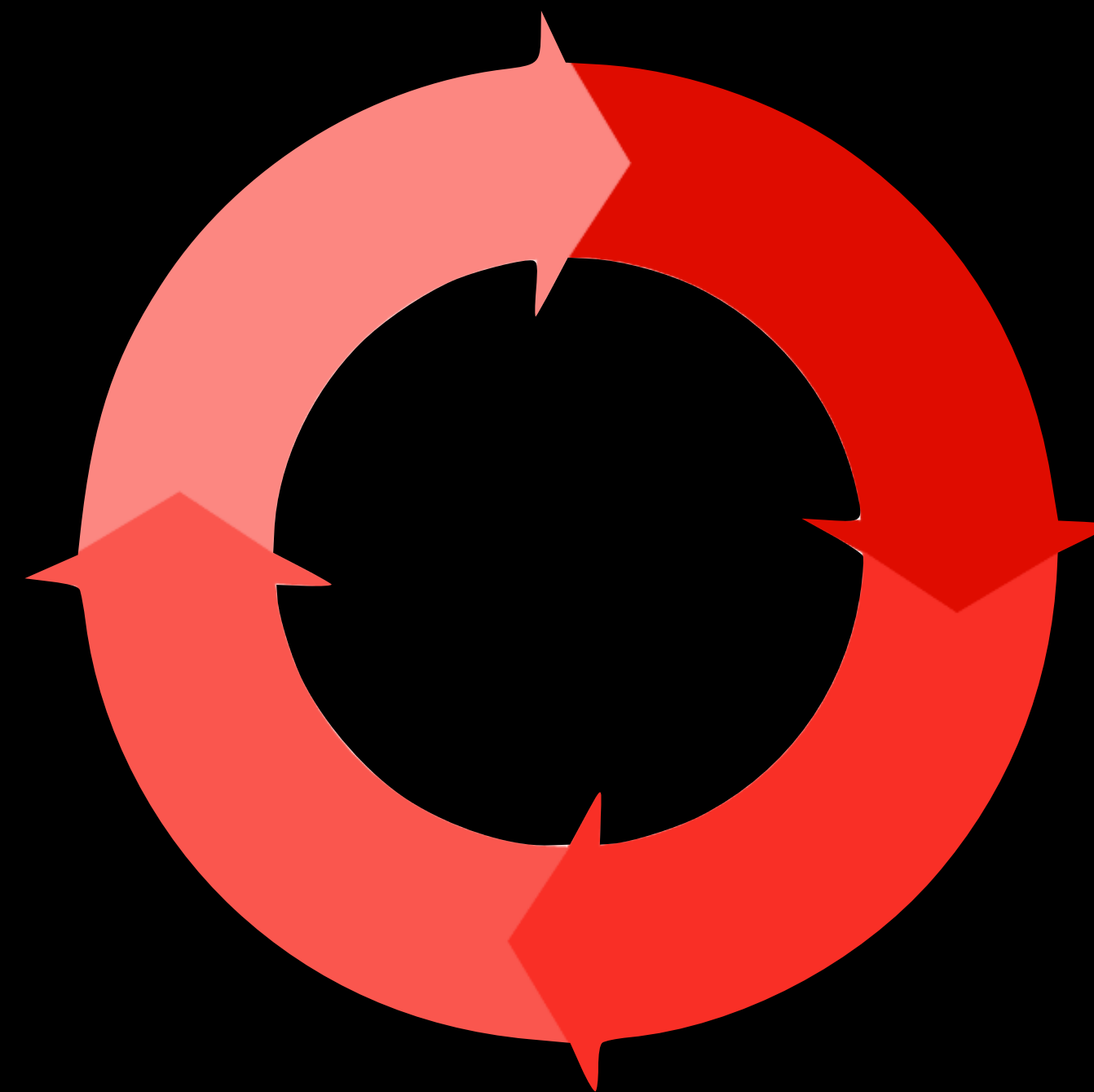
2020/11/10



2021/10/20



2022/10/20





Shipped: 10/07/19
mSCP: 10/06/20
CIS: 04/06/20
STIG: 07/31/20

11/12/20
11/10/20
03/02/21
11/20/20

10/25/21
10/20/21
12/03/21
02/03/22

10/24/22
10/20/22
11/16/22
04/24/23



Release Ready



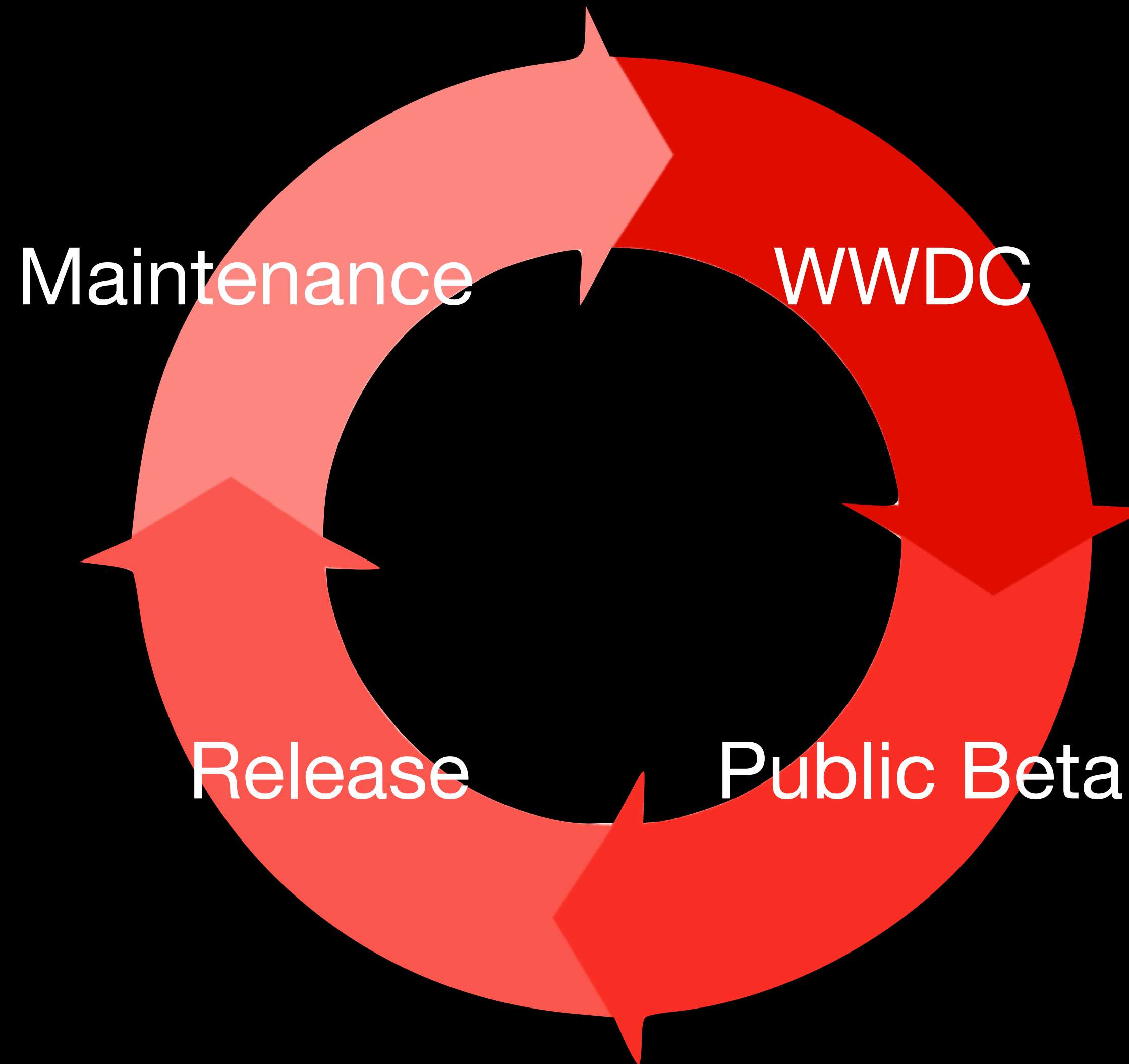
New Release/Guidance



New Hardware



Lifecycle



NIST SP 800-53
Revision 4



NIST SP 800-53
Revision 5



CIS Critical Security
Controls Version 8



Why does all this matter?

CISA

- BOD 22-01
- BOD 23-01

Executive Order

- EO 14028

OMB Memorandum

- M-21-31



Why does all this matter?



“We’re required to use the DISA STIG for compliance, the mSCP has taken that from a nearly impossible task to one that is very easy to do.”

John Daly - Naval Air Warfare Center

“The mSCP makes a daunting task approachable for Mac Admins of all skill levels, creating easy to comprehend reports for InfoSec and Auditors.”

**Jordan Burnette -
Virginia Commonwealth University**

“We’re a small team of two supporting a few hundred Macs, without mSCP, we likely would have fallen behind on many other projects or had to hire additional team members to support us.”

Niko Torres - New Teacher Center

“The mSCP has saved countless man hours creating and auditing security policies on our Macs. InfoSec thinks I’m a super hero!”

Lee Stanford - Workhuman

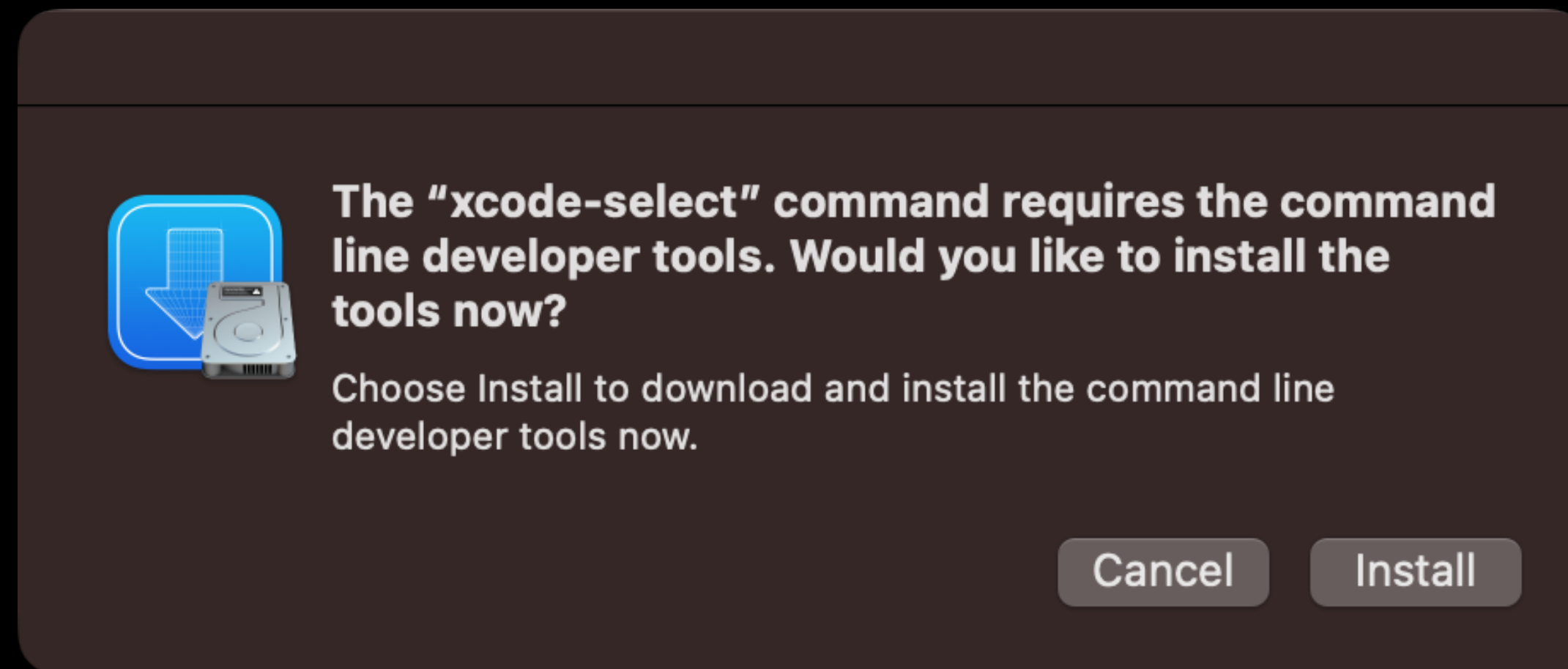


Endpoint Requirements




















mac
OS



mSCP Requirements



main 14 branches 20 tags Go to file Code

 robertgndler Merge branch 'ventura'	10705d9 on Dec 8, 2022	🕒 1,034 commits
 .github/ISSUE_TEMPLATE	Merge branch 'ventura'	7 months ago
 baselines	changed 12 to 13 in title	6 months ago
 build	Initial content commit	3 years ago
 custom	Initial content commit	3 years ago
 includes	fix[helperfile] fixed mscp-data file	5 months ago
 rules	refactor[rules] CCEs added	5 months ago
 scripts	feat[script] Additional Authors	6 months ago
 sections	refactor[smartcards] Added info on ignoreARD key	8 months ago
 templates	fix[helperfiles] updated adoc_additional_docs	5 months ago
 .gitattributes	Create .gitattributes	3 years ago
 .gitignore	added ruby gem changes	10 months ago
 CHANGELOG.adoc	Updated 1.1 date	5 months ago
 CONTRIBUTING.adoc	Create CONTRIBUTING.adoc	3 years ago
 Gemfile	fix[helperfile] Set version for Rogue	5 months ago
 LICENSE.md	Create LICENSE.md	3 years ago
 README.adoc	Update README.adoc	7 months ago
 VERSION.yaml	refactor[rules,docs]: final updates for release	5 months ago
 requirements.txt	yaml no longer required	2 years ago

About

macOS Security Compliance Project

- macos
- bash
- zsh
- apple
- python3
- compliance
- mdm

- 📖 Readme
- 📄 View license
- ★ 1.2k stars
- 👁 114 watching
- 🍴 146 forks

Report repository

Releases 20

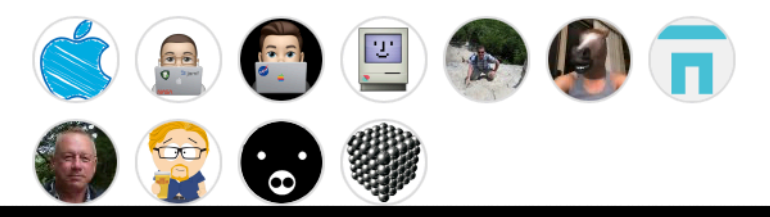
Ventura Guidance Revision 1.1 Latest on Dec 8, 2022

+ 19 releases

Packages

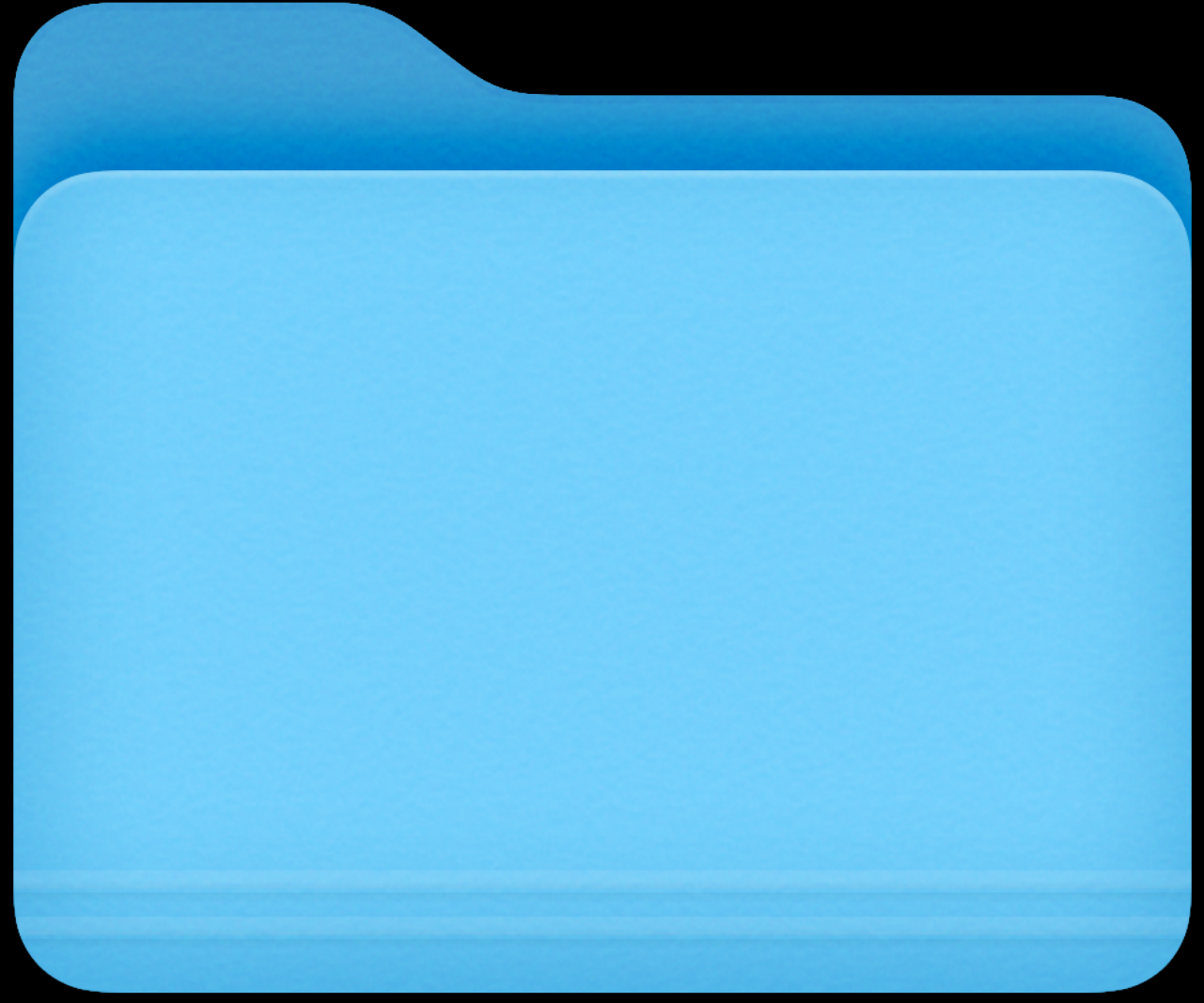
No packages published

Contributors 11





Rules



Baselines



Scripts



generate_guidance.py



generate_baseline.py

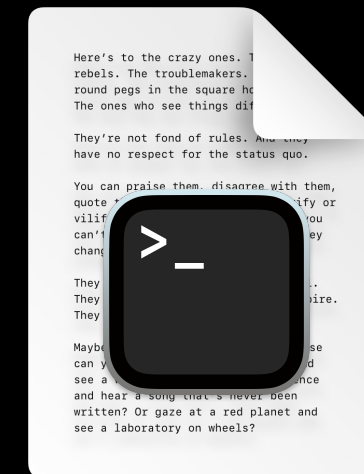


generate_mapping.py



generate_scap.py

Project Outputs



DEMO

Security Compliance Project

One More Thing...

