StateRAMP

STATERAMP OVERVIEW

October 5, 2022

Speaker

Leah McGrath
Executive Director
StateRAMP

leah@stateramp.org

Leah dedicated more than 1,000 hours in 2020 working alongside Steering Committee members to develop StateRAMP's governance and policy framework, and now serves as the non-profit's first executive director.

Prior to her work with StateRAMP, Leah held leadership positions in both the public and private sector, including serving as the first deputy mayor of the City of Fishers, Indiana from 2015 - 2019.

Agenda

What is StateRAMP

- History
- How does it work for Providers
- How does it work for Government

How to Get Started with StateRAMP

Next Steps

About StateRAMP

As cyber threats grow, how do you know…

If a cloud solution is being used to deliver services that transmits, stores, processes and/or ***could impact security*** of Government data?

Bidders meet minimum security standards ***before*** making an award for contract?

Contracted vendor complies with your security standards ***throughout contract*** duration?

StateRAMP

RISK & AUTHORIZED MANAGEMENT PROGRAM

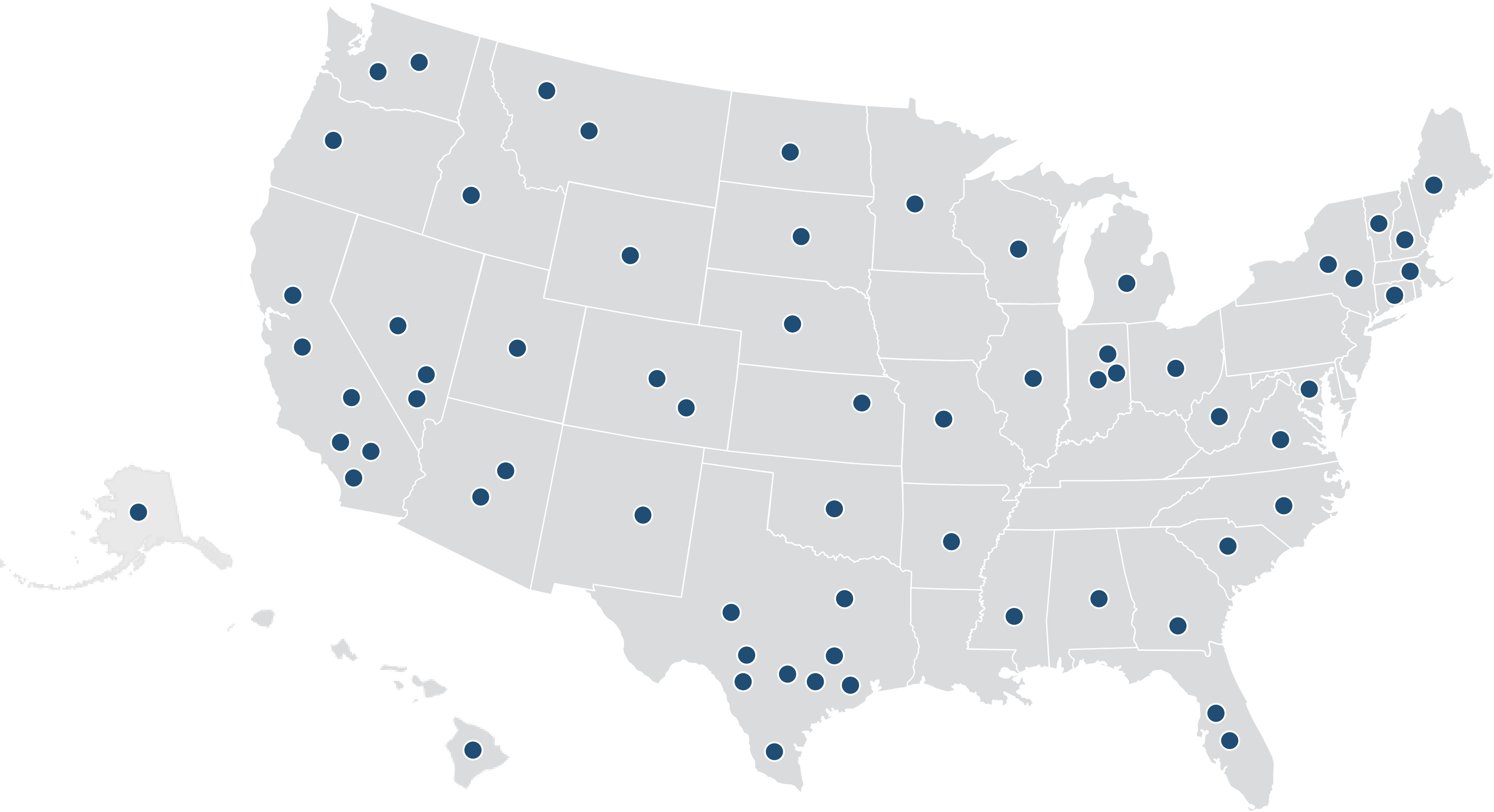
StateRAMP is a non-profit, 501c6, membership organization that brings together state and local governments, educational institutions, and special districts with the providers who serve them to promote best cyber practices and to establish a common set of security criteria.

A standard method of verifying cloud security:

- Allows providers to verify product’s security posture once to prove their cybersecurity compliance to all their government clients.
- Provides governments a shared resource for procurement and continuous compliance & monitoring.

Learn more at *www.stateramp.org*

StateRAMP Members



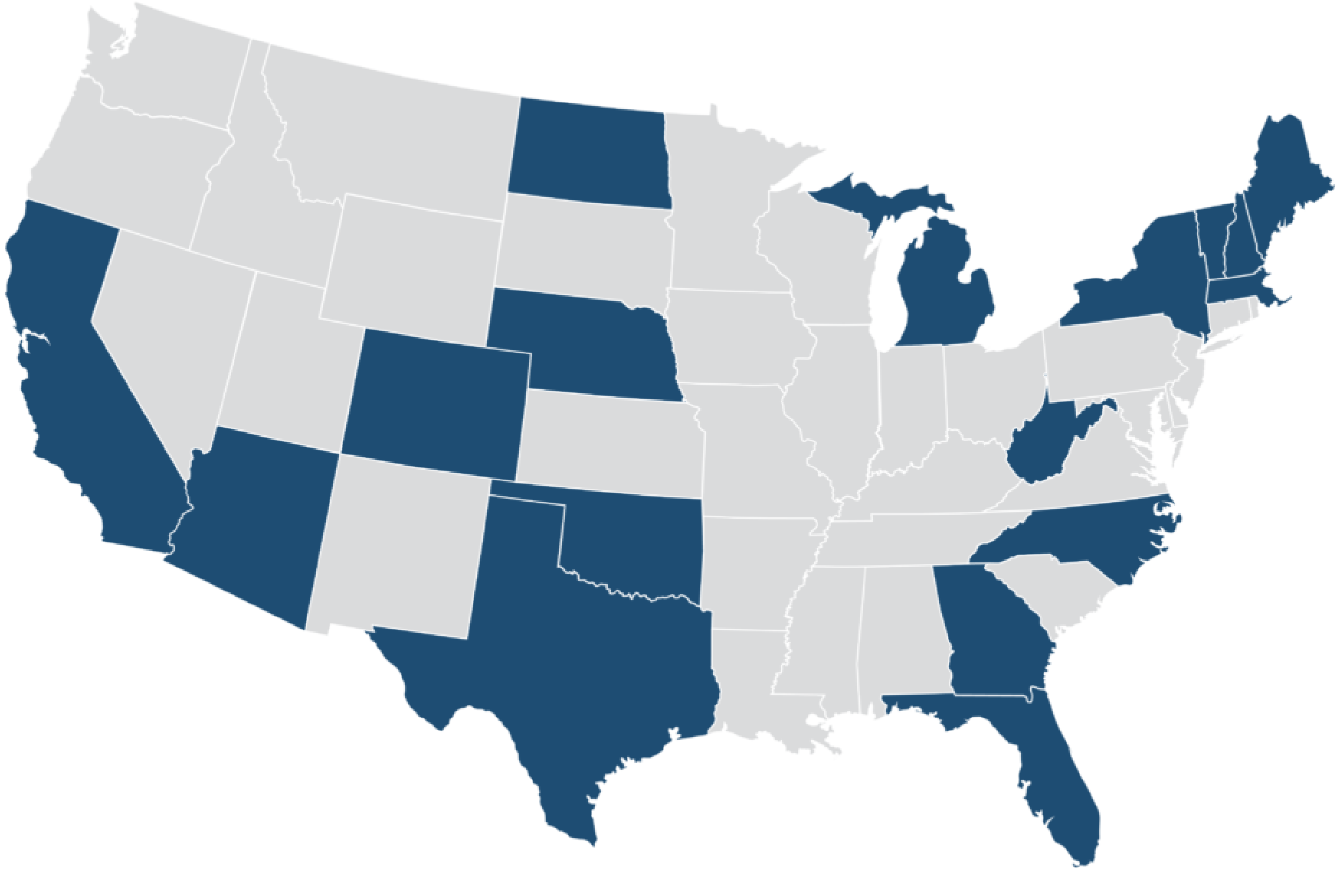
295 Individual Govt. Members
111 Provider Members

Government & Providers may join at
www.stateramp.org/register

*As of September 30, 2022

Growing Government Participation

Arizona
Arkansas (Judicial)
California
Colorado
Florida
Georgia
Maine
Massachusetts
Michigan
Nebraska (Judicial)
New Hampshire
North Carolina
North Dakota
Oklahoma
Texas
Vermont
West Virginia



Emerging Higher Ed + Local Government:
New York State Local Government IT Directors' Association, UNC System, Sacramento County + More

How it Works & Security Requirements

StateRAMP

Board of Directors & Steering Committee

J.R. Sloan
CIO
State of Arizona

Ted Cotterill
CPO / General Counsel
State of Indiana

Joe Bielawski
President
Knowledge Services

Rich Banta
CISO &
Managing Partner
Lifeline Data Centers

Tony Bai
Federal Practice Lead
A-LIGN

Paul Baltzell
Vice President
Strategy & Bus. Dev.
Salesforce

Curtis Dukes
Executive VP
Center for Internet
Security

Dan Lohrmann
Chief Strategist &
CISO
Security Mentor

Steve Nettles
Procurement
Group Mgr.
State of Arizona

Jason Oksenhendler
Sr. Mgr., Cyber Security
Coalfire

Dugan Petty
Advisor
Retired CIO / CPO

Doug Robinson
Executive Director
NASCIO

Tim Roemer
Dir. Homeland
Security + CISO
State of Arizona

Jaime Schorr
Chief Procurement Officer
State of Maine

Teri Takai
Vice President
Center for Digital Govt.

Fay Tan
Coop. Contract Coord.
NASPO ValuePoint

Paul Toomey
CEO
Geographic Solutions

Jay White
CISO
State of Mississippi

Owen Zorge
CISO
City of Chandler, AZ

Not pictured: Tom Considine, Sr., Sr. InfoSec/AZRamp, State of Arizona

Standing Committees

Standards & Technical

Dan Lohrmann, Chair
Chief Strategist & Chief Security Officer
Security Mentor

Nancy Rainosek, Vice Chair
Chief Information Security Officer, State of Texas

Members:
David Allen *(Georgia)*
Glenn Herdrich *(Sacramento Co.)*
Steve Nettles *(Arizona)*
Jason Oskenhendler *(Coalfire)*
Joe Bielawski *(Board Member)*

Advisors:
Phyllis Lee *(Ctr Internet Security)*
Rick Zak *(Microsoft)*
Maria Thompson *(AWS)*
Noah Brown *(StateRAMP PMO)*

Appeals

Owen Zorge, Chair
State Compliance & Privacy Ofc
City of Chandler, AZ

Rich Banta, Vice Chair
Co-owner & CISO,
Lifelines Data Center

Members:
Chance Grubb *(Oklahoma)*
Ted Cotterill *(Board Member)*
Teri Takai *(Ctr for Digital Govt)*

Advisors:
Tony Bai *(A-LIGN)*
Mase Izadjoo *(Earthling Security)*

Approvals

David Allen, Chair
Chief Information Security Officer
State of Georgia

Members:
Jayson Cavendish *(Michigan)*
Rob Main (*North Carolina)*
Adam Mikeal (*Texas A&M University)*
Antoine Charles (*Oklahoma)*

Nominating

Jaime Schorr, Chair
Chief Procurement Officer
State of Maine

Members:
Fay Tan (*NASPO ValuePoint)*
Doug Robinson *(NASCIO)*
Dugan Petty *(Advisor)*
J.R. Sloan *(Board Member)*
Jay White *(Mississippi)*
Paul Baltzell *(Salesforce)*

Templates & Resources

Governance committees adopt policies that define

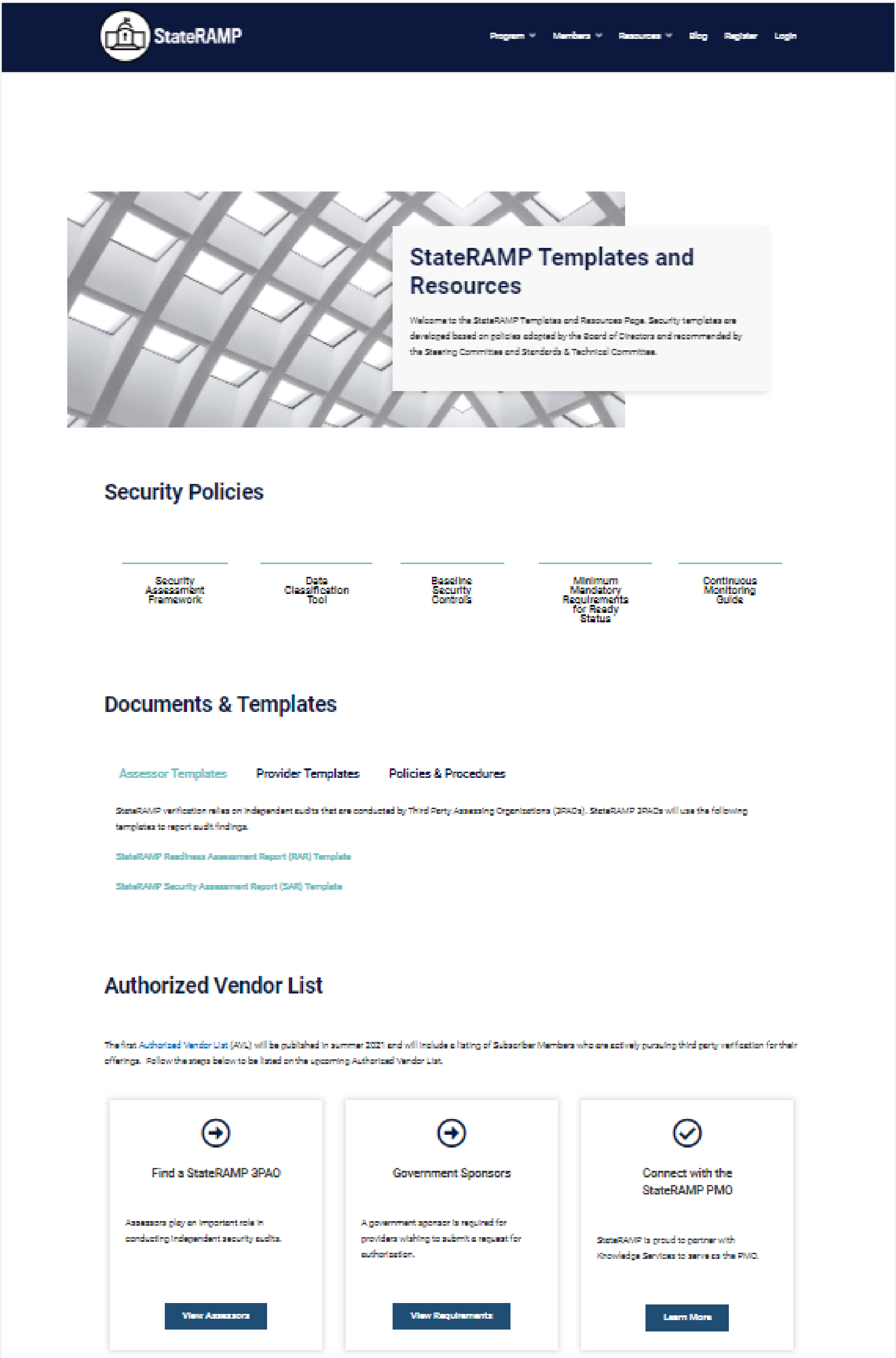
- Baseline minimums standards
- Process for StateRAMP verification

Baseline requirements built on NIST 800-53 Rev. 4

- Rev. 5 in 2023
- Goal to map frameworks for CJIS, MARSE/MMIS/HIPAA and more

Find policies, templates and resources online

- www.stateramp.org/templates-resources



StateRAMP Templates and Resources

Welcome to the StateRAMP Templates and Resources Page. Security templates are developed based on policies adopted by the Board of Directors and recommended by the Steering Committee and Standards & Technical Committee.

Security Policies

Security Assessment Framework
Data Classification Tool
Baseline Security Controls
Minimum Mandatory Requirements for Ready Status
Continuous Monitoring Guide

Documents & Templates

StateRAMP verification relies on independent audits that are conducted by Third Party Assessing Organizations (3PAOs). StateRAMP 3PAOs will use the following templates to report audit findings.

StateRAMP Readiness Assessment Report (RAR) Template

StateRAMP Security Assessment Report (SAR) Template

Authorized Vendor List

The first Authorized Vendor List (AVL) will be published in summer 2021 and will include a listing of Subscriber Members who are actively pursuing third party verification for their offerings. Follow the steps below to be listed on the upcoming Authorized Vendor List.

Find a StateRAMP 3PAO

Assessors play an important role in conducting independent security audits.

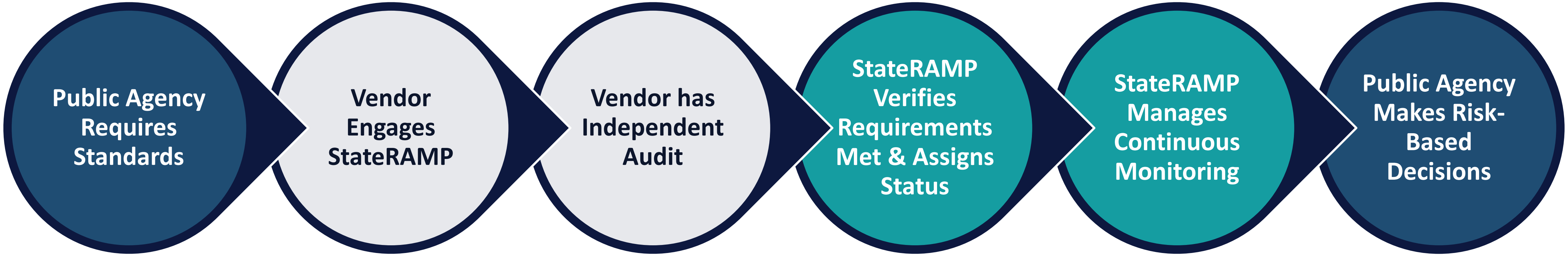
Government Sponsors

A government sponsor is required for providers wishing to submit a request for authorization.

Connect with the StateRAMP PMO

StateRAMP is proud to partner with Knowledge Services to serve as the PMO.

StateRAMP Verification Process



Public Agency Requires Standards

Vendor Engages StateRAMP

Vendor has Independent Audit

StateRAMP Verifies Requirements Met & Assigns Status

StateRAMP Manages Continuous Monitoring

Public Agency Makes Risk-Based Decisions

Verify Cloud Products Used by Public Agencies Meet Minimum Security RequirementsOngoing

- Standardized Requirements (Based on NIST 800-53)
- Independent Annual Audits
- Centralized Program Management Office (PMO)
- Continuous Monitoring (Monthly Reporting + Annual Audit)

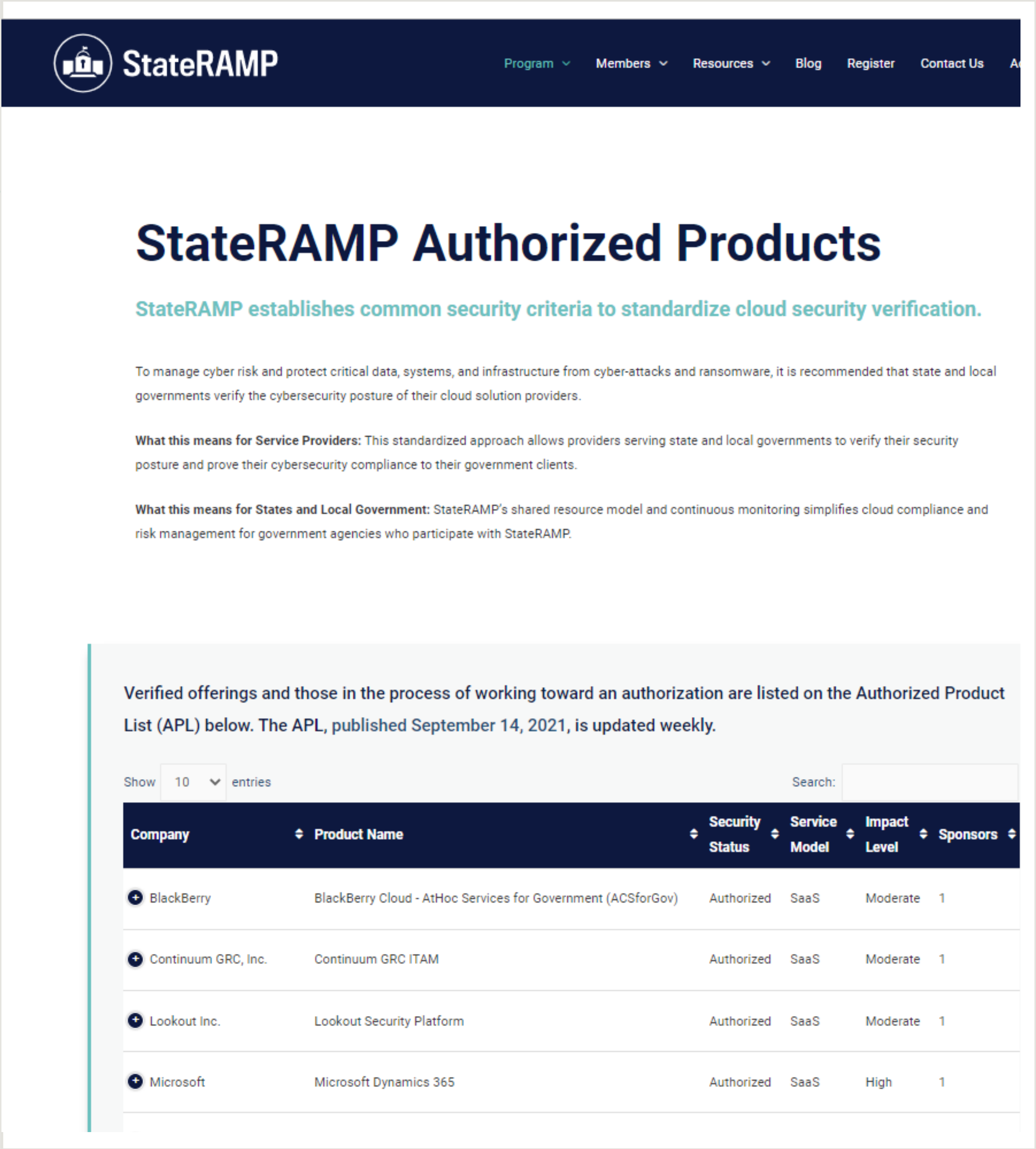
Authorized Product List (APL)

Public list on www.stateramp.org

Recognize progressing and verified statuses

Continuous monitoring is required to maintain a verified listing (Ready, Authorized, and Provisional)

Participating StateRAMP Governments provided secure access to portal to view continuous monitoring



StateRAMP Authorized Products

StateRAMP establishes common security criteria to standardize cloud security verification.

To manage cyber risk and protect critical data, systems, and infrastructure from cyber-attacks and ransomware, it is recommended that state and local governments verify the cybersecurity posture of their cloud solution providers.

What this means for Service Providers: This standardized approach allows providers serving state and local governments to verify their security posture and prove their cybersecurity compliance to their government clients.

What this means for States and Local Government: StateRAMP's shared resource model and continuous monitoring simplifies cloud compliance and risk management for government agencies who participate with StateRAMP.

Verified offerings and those in the process of working toward an authorization are listed on the Authorized Product List (APL) below. The APL, published September 14, 2021, is updated weekly.

Show 10 entries Search:

Company	Product Name	Security Status	Service Model	Impact Level	Sponsors
BlackBerry	BlackBerry Cloud - AtHoc Services for Government (ACSforGov)	Authorized	SaaS	Moderate	1
Continuum GRC, Inc.	Continuum GRC ITAM	Authorized	SaaS	Moderate	1
Lookout Inc.	Lookout Security Platform	Authorized	SaaS	Moderate	1
Microsoft	Microsoft Dynamics 365	Authorized	SaaS	High	1

Security Status Progression

Meets minimum mandatory requirements and submits a completed 3PAO Readiness Assessment Report (SR-RAR).

Requires Sponsor or Approvals Committee Support; Meets requirements by impact level and submits completed 3PAO Security Assessment Plan (SR-SAP) and documentation.

Requires Sponsor; Meets minimum requirements for Ready; but not all for Authorized; Sponsor may assign Provisional Status.

StateRAMP Impact Levels

Government entity defines required procurement/contract security impact level.
StateRAMP Impact Level Categories align to NIST 800-53 Rev. 4 (Rev. 5 in 2023).

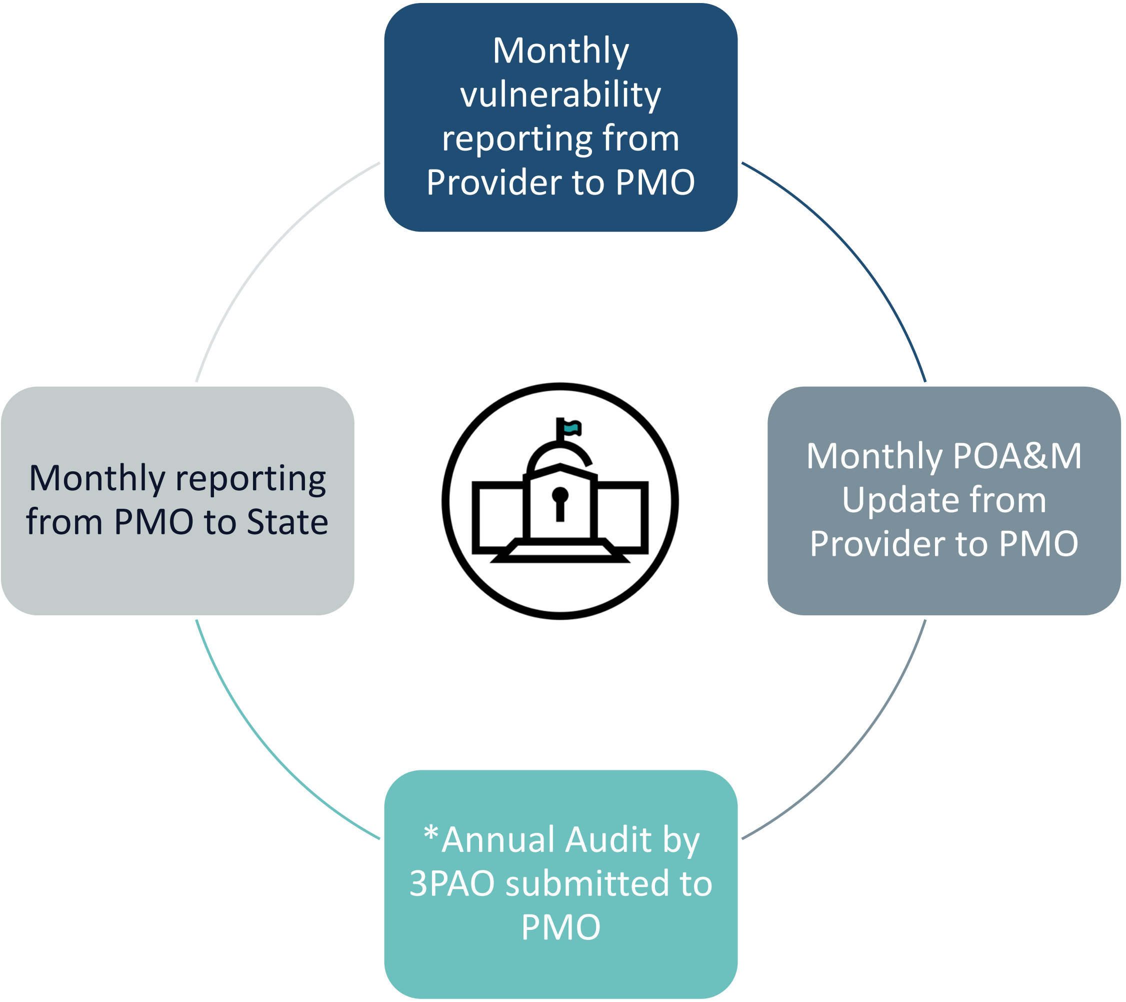
Low	**Low+**	**Moderate**	**High**
StateRAMP Low Control Baselines	StateRAMP Low+ Control Baselines	StateRAMP Moderate Control Baselines	FedRAMP High Control Baselines

View Data Classification Tool at: www.stateramp.org/templates-resources.

StateRAMP and FedRAMP

https://stateramp.org/blog/

	StateRAMP	FedRAMP
Based on NIST 800-53 Rev. 4	✓	✓
Requires annual independent Third Party Assessment Organization (3PAO) Audit	✓	✓
Requires Monthly Continuous Monitoring	✓	✓
Impact Levels of Low, Moderate, and High	✓	✓
Verified statuses of Ready and Authorized	✓	✓
Available to any provider, regardless of federal contract status	✓	
Documentation available to federal, state, local, public education institutions, and special districts	✓	
Centralized PMO reviews all security packages to ensure consistent application of standards and verification	✓	
Fast Track option for products with FedRAMP or StateRAMP	✓	
Plans for mapping to other compliance frameworks: CJIS, MARSE, MMIS, IRS	✓	
Nonprofit mission to improve cyber posture for state, local, public education institutions and special districts and providers who serve them	✓	



Monthly vulnerability reporting from Provider to PMO

Monthly POA&M Update from Provider to PMO

*Annual Audit by 3PAO submitted to PMO

Monthly reporting from PMO to State

Continuous Monitoring

Providers must comply with Continuous Monitoring requirements to maintain status Ready, Authorized or Provisional

View Continuous Monitoring Policies & Escalation Process for more: www.stateramp.org/templates-resources.

Getting Started

Become a Member of StateRAMP

Government Membership

Individual + Certified Government Membership

No Cost to Government

www.stateramp.org/register

Schedule a call for your team:

Rebecca@stateramp.org

Provider Membership

Provider Membership

$500 Annual Membership Fee

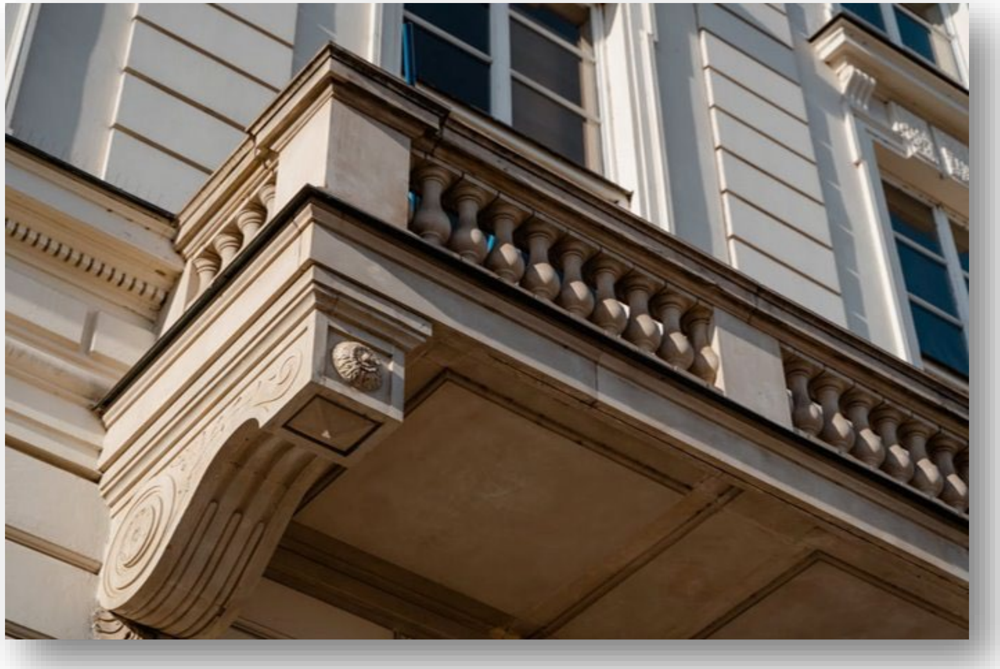
www.stateramp.org/register

Schedule a call for your team:

info@stateramp.org

View ***Getting Started Guides*** for Government and Providers at www.stateramp.org

Government Adoption Support



Schedule a meeting! Email info@stateramp.org.

StateRAMP Implementations Team Support

- Overall Procurement Implementation
- Overall InfoSec Implementation
- Onboarding to PMO Portal for ConMon
- Solicitation and Contract Language
- Education and Training
- Vendor Outreach
- Reporting and Communication

Coming Soon: Bridge to StateRAMP

StateRAMP Security Snapshot

- StateRAMP will make available to providers and governments a new “pre-Ready” assessment, known as the StateRAMP Security Snapshot.
  - Available for products not yet achieved a verified security status of StateRAMP Ready, Authorized or Provisional
  - Snapshot to include a score that assesses the level of cyber maturity of the product in relation to achieving StateRAMP Ready

- Help bridge the transition to StateRAMP for providers and governments.
  - May be incorporated into solicitation requirements to provide governments an ability to assess NIST maturity upfront, while providers work to achieve StateRAMP authorization.

StateRAMP Security Snapshot in Procurement Process

Steps for Getting Started

1. Identify Security Impact Level Required (Use StateRAMP Data Classification Tool)
2. Require StateRAMP Security Snapshot Score as a Deliverable for Solicitation Response that is No Older than 6 Months at Submission. StateRAMP Ready, Authorized or Provisional Certifications exceed this requirement.
3. Require updated StateRAMP Security Snapshot within 6 months after Contract Execution (Note: This will demonstrate whether progress is being made toward StateRAMP authorization.)
4. Require StateRAMP Ready within 12 months of Contract Execution (Continuous Monitoring Begins)
5. Require StateRAMP Provisional/Authorized within 18 Months of Contract Execution

Sample Language

SECURITY FRAMEWORK & CONTRACTOR REQUIREMENTS
The State information security policies and standards adhere to the National Institute of Standards and Technology (NIST) 800-53 revision 4 (or latest version adopted by StateRAMP).

A contract will not be executed with a contractor that utilizes a cloud system to process, store and/or transmit government data, unless and until the service provider has achieved StateRAMP Ready Status. The Ready Status serves as an attestation to the providers capabilities to achieve full authorization.

The State requires all cloud systems that process, store and/or transmit government data must demonstrate compliance with NIST 800-53 at StateRAMP Impact Level (Low/Moderate/High/Specific State Requirements) by achieving StateRAMP authorization within 12 months of contract execution for the appropriate data classification.

Once a contract is issued, the provider must achieve full StateRAMP authorization within twelve (12) months. All contractors must comply with required continuous monitoring to maintain StateRAMP authorizations.

The State reserves the right to request and review all Third-Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and penetration tests of the contractor’s environment. The contractor shall respond to all flaws discovered by providing an acceptable timeframe to resolve the issue and/or implement a compensating control.

Any deviation from these requirements must be approved by the Chief Information Officer. Information about StateRAMP can be found at www.stateramp.org.

Resources

Helpful Links

www.stateramp.org

Get Started as a Participating Government: rebecca@stateramp.org

Join as an Individual Government Member: www.stateramp.org/register

Join as a Provider Member: www.stateramp.org/register

Security Policies & Templates: www.stateramp.org/templates-resources

Governance & Documents: www.stateramp.org/documents

Request a Security Review for Ready or Authorized: www.stateramp.org/providers

Future Events: www.stateramp.org/events

Blogs: www.stateramp.org/blog

StateRAMP

LEAH MCGRATH

EXECUTIVE DIRECTOR

LEAH@STATERAMP.ORG

Common FAQ

SOC 2 v. StateRAMP Audits

SOC 2

A SOC 2 report is a measurement against self-established security controls, procedures, and policies.

SOC 2 is a framework designed by financial experts of the American Institute of CPAs and "is intended to meet the needs of a broad range of users."

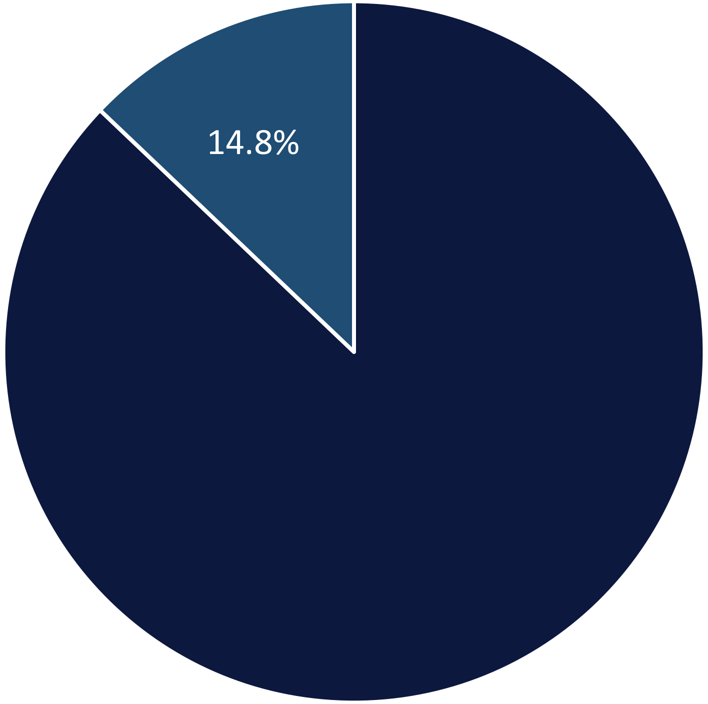
STATERAMP

StateRAMP compliance is a measurement against a standard set of security controls, procedures, and policies established by the StateRAMP Committees.

StateRAMP requirements are designed by cyber security professionals specifically to measure compliance with NIST 800-53 for State and Local Government.

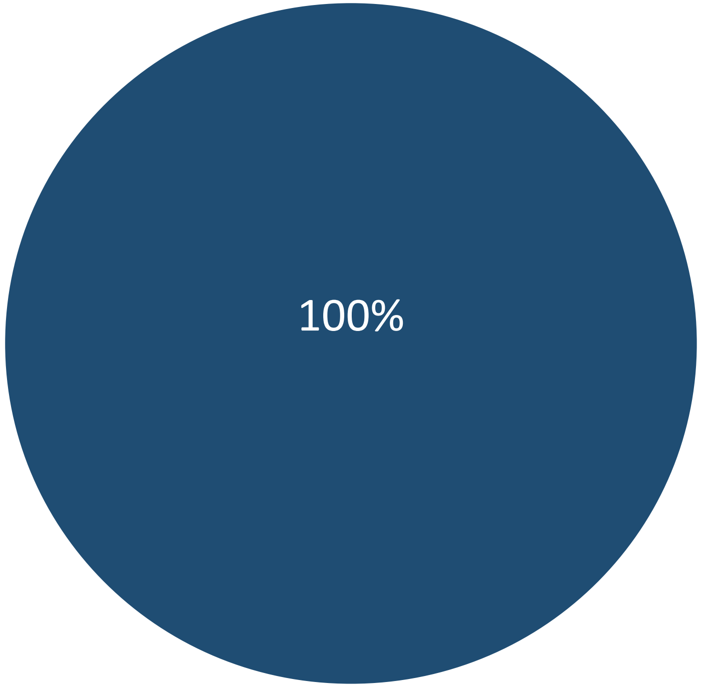
StateRAMP v. SOC 2 Audits for NIST 800-53

SOC 2 NIST 800-53 Compliance



*Assumes audited CSP selects all 42 NIST Controls for audit

StateRAMP NIST 800-53 Compliance



*StateRAMP audits are the same every time. Control requirements vary only by Impact Level.

Implementation Requirements are Critical

SOC 2 is a framework, not a control catalog. As such, its controls are not descriptive and allow interpretation of implementation.

- StateRAMP and FedRAMP have specific requirements and implementations for NIST 800-53 controls.
- The gap in SOC 2 coverage of NIST 800-53 controls is due to the lack of implementation requirements.

See following slides for example of differing requirements and impact.

Example of Differing Requirements

Below is an example of differing requirements for Access Control related to Password Requirements.

SOC 2 requires self-definition, while StateRAMP requires specific NIST 800-53 compliance.

SOC 2

"Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian."

StateRAMP

NIST: "The information system, for password-based authentication:

(a) Enforces minimum password complexity of case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters;

(b) Enforces at least the following number of changed characters when new passwords are created: at least one

(c) Stores and transmits only encrypted representations of passwords;

(d) Enforces password minimum and maximum lifetime restrictions of one day minimum, sixty day maximum;

(e) Prohibits password reuse for twenty four generations; and

(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password."

Example of Differing Requirements

This chart illustrates the difference in password compliance for audits.

Requirement	StateRAMP / NIST	SOC 2
Defined number of characters	12	None
Required Upper Case Letters	At least one	None
Required Lower Case Letters	At least one	None
Required Numbers	At least one	None
Required Special Characters	At least one	None
Requires new password to not be the same as old password?	Yes	No
Password transmission must be encrypted	Yes	No
Minimum age of password	1 Day	None
Maximum age of password	60 days	None
Prohibit password re-use	24 generations	None

Impact of Differing Requirements on Compliance

In this example, password compliance differs significantly.

SOC 2

Compliant IF:

Define a password as being four numbers

Requirement self-defined

StateRAMP

Compliant IF:

Password has “minimum of 12 characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters, one character change with each password changes, only transmit passwords encrypted, require lifetime restriction of one-day minimum and 60-day maximum, and prevent reuse of the previous 24 passwords”

Requirement set by NIST 800-53

Impact of Differing Requirements on Risk

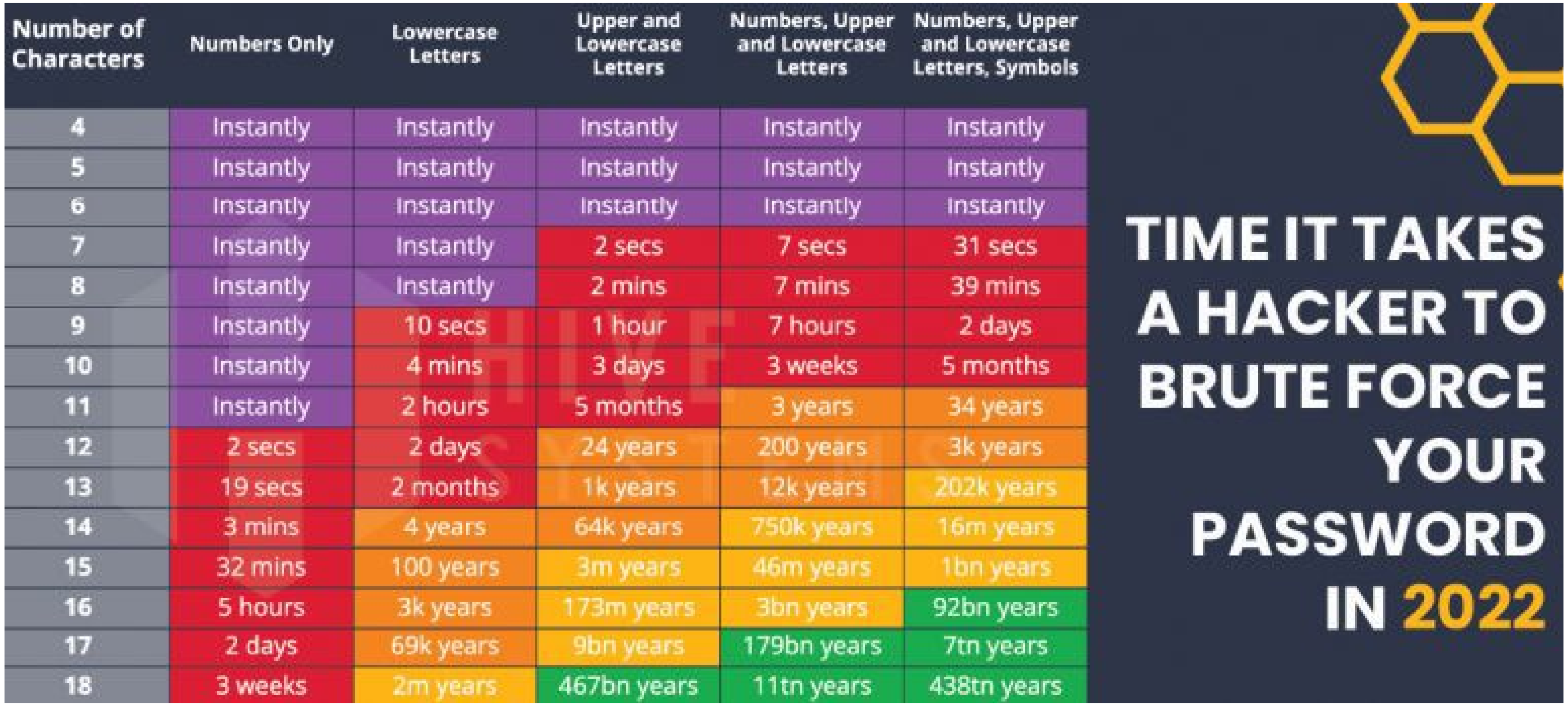
More importantly, in this example, risk differs significantly.

SOC 2

4 Digit Password could be cracked instantly with brute force

StateRAMP

NIST Password would take 3,000 years



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Image: Hive Systems