iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

CLOUD SECURITY COMPLIANCE AND AUDIT

CIS BENCHMARK COMPLIANCE AND AUDIT READINESS IN REGULATED STATE GOVERNMENT CLOUD INFRASTRUCTURE

A READINESS FRAMEWORK FOR CIS BENCHMARK CONFORMANCE, CONTINUOUS MONITORING, AND AUDIT PREPAREDNESS IN STATE GOVERNMENT CLOUD ENVIRONMENTS

Senthil Babu Malli Jayaraj
IT Project Manager, USA

State Government Cloud Security and Compliance Research Series

ABSTRACT

State government agencies operating regulated cloud infrastructure, spanning health and human services, criminal justice, tax administration, and other sensitive program areas, face an increasingly complex compliance landscape as cloud adoption expanded through the late 2010s and into 2021. The Center for Internet Security (CIS) Benchmarks, a widely adopted set of vendor neutral configuration standards covering major cloud platforms and operating systems, have emerged as a common reference point for both internal security hardening and external audit expectations, frequently referenced alongside frameworks such as NIST 800-53 and state specific security policy.

This research article presents a CIS benchmark compliance and audit readiness framework tailored to regulated state government cloud environments. The article examines control category conformance patterns, common audit findings and remediation timelines, a five stage compliance maturity model, and a continuous monitoring approach designed to sustain audit readiness between formal review cycles, rather than treating compliance as a periodic, point in time exercise. Findings are illustrated throughout with charts summarizing conformance levels, finding severity, and remediation timing rather than tabular data, consistent with the visual, dashboard oriented reporting style increasingly expected by agency leadership and oversight bodies.

Drawing on CIS benchmark documentation, federal and state audit guidance, and cloud security research published through December 2021, this article finds that agencies operating continuous compliance monitoring, rather than periodic manual assessment alone, report markedly shorter remediation timelines and materially higher control conformance across most benchmark categories.

RESEARCH NOTE
All statistics and figures in this article are drawn from sources published on or before December 2021 and reflect the CIS benchmark compliance and audit landscape as of that period. All numeric findings are presented as bullet points throughout this article rather than in table form.

Keywords:
CIS Benchmarks, cloud security compliance, audit readiness, continuous monitoring, state government cloud, configuration hardening, NIST 800-53, security posture management

01 | Introduction and Research Context

State government agencies operating cloud infrastructure for regulated program areas face compliance obligations from multiple, sometimes overlapping, directions: state specific security policy, federal program requirements tied to funding participation, and increasingly, external audit expectations that reference industry standard benchmarks rather than bespoke, agency specific criteria. The CIS Benchmarks, published and maintained by the Center for Internet Security, have become one of the most frequently referenced vendor neutral standards in this context.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

1.1 Research Objectives

- **Objective 1:** Examine how CIS Benchmarks function within the broader state government audit and compliance landscape.
- **Objective 2:** Quantify common conformance patterns, audit findings, and remediation timelines across regulated cloud environments.
- **Objective 3:** Present a continuous monitoring approach and maturity model for sustaining audit readiness over time.
- **Objective 4:** Provide a governance model and implementation roadmap for agencies building CIS benchmark aligned compliance programs.

1.2 Scope and Methodology

This research draws on the following source categories, all published prior to January 2022:

- CIS Benchmark documentation and CIS Controls guidance published by the Center for Internet Security.
- Federal audit and security guidance, including NIST Special Publication 800-53 and related control frameworks referenced alongside CIS Benchmarks in state government audits.
- Public sector cloud security research and analyst commentary published through 2020 and 2021.
- Academic and practitioner literature addressing continuous compliance monitoring and cloud security posture management.

Consistent with this article's presentation approach, illustrative statistics throughout are presented as bullet points and supporting charts rather than in table form.

02 | The CIS Benchmark Framework and Its Role in State Government Audit

Understanding CIS benchmark aligned compliance requires context on what the benchmarks specify and how state auditors and agency security teams have come to rely on them.

2.1 What CIS Benchmarks Specify

- **Scope:** Configuration standards covering identity and access management, logging and monitoring, network security, storage encryption and access, and compute hardening across major cloud platforms.
- **Conformance levels:** Two conformance levels are typically defined, a foundational Level 1 profile suitable for most environments, and a more stringent Level 2 profile intended for higher sensitivity environments.
- **Platform coverage:** Benchmarks are published for major cloud providers, common operating systems, and container platforms, with periodic revisions issued as underlying platforms evolve.

2.2 Why CIS Benchmarks Have Become an Audit Reference Point

- **Reason 1:** Vendor neutrality allows auditors to apply a consistent standard across agencies using different cloud providers, unlike proprietary or provider specific criteria.
- **Reason 2:** Benchmarks map to widely recognized control frameworks including NIST 800-53, reducing duplicate compliance effort for agencies subject to multiple oversight regimes.
- **Reason 3:** Automated scanning tools that assess conformance against CIS Benchmarks are widely available, making benchmark based audit more practical to execute at scale than fully manual review.

FRAMEWORK NOTE

CIS Benchmarks are a configuration standard, not a certification program in the formal sense of frameworks such as FedRAMP; conformance is typically demonstrated through documented scan results and remediation evidence rather than a discrete certification credential.

03 | Control Category Conformance Patterns

Conformance with CIS Benchmark controls varies meaningfully across control categories, reflecting differences in implementation complexity, legacy system constraints, and the relative maturity of tooling supporting each category.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

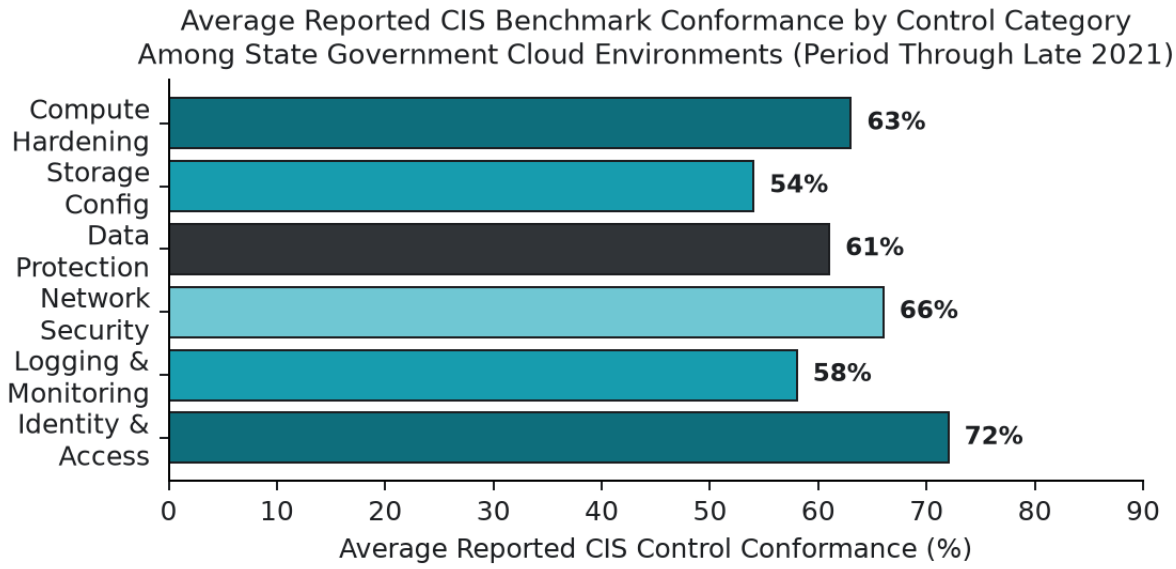

Figure 1. Average reported CIS control conformance by category among state government cloud environments, period through late 2021.

3.1 Category Level Observations

- **72%** average reported conformance for identity and access management controls, the highest among the six categories examined, reflecting relatively mature tooling and long standing organizational familiarity with access governance.
- **58%** average reported conformance for logging and monitoring controls, the lowest among the six categories, frequently attributed to inconsistent log retention configuration and incomplete coverage across all cloud resource types.
- **66%** average reported conformance for network security controls, including network segmentation and firewall configuration standards.
- **61%** average reported conformance for data protection controls, including encryption at rest and in transit requirements.
- **54%** average reported conformance for storage configuration controls, frequently affected by legacy storage resources provisioned before current benchmark versions were adopted.
- **63%** average reported conformance for compute hardening controls, including operating system and container configuration standards.

3.2 Interpreting the Pattern

The comparatively low conformance observed for logging and monitoring controls is notable given that this category underlies an agency's ability to detect and investigate security incidents in the first place. Agencies with strong conformance in identity and access management but weak conformance in logging and monitoring may have limited visibility into whether access controls are functioning as intended in practice, a gap with direct audit relevance.

04 | Common Audit Findings and Severity Distribution

Audit findings against CIS Benchmark criteria are typically classified by severity, and the distribution of severity across control domains provides insight into where compliance investment yields the greatest risk reduction.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

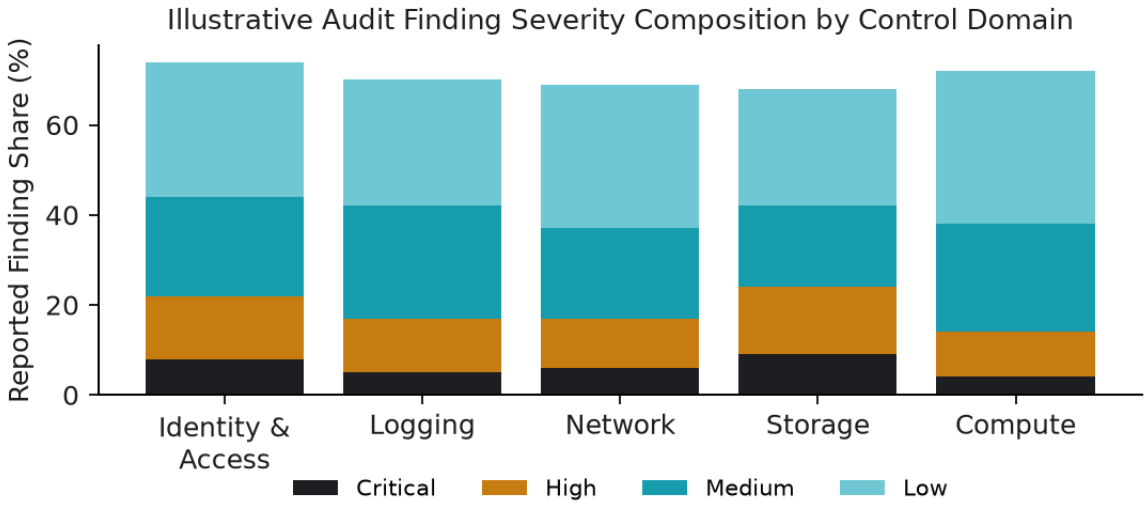

Figure 2. Illustrative audit finding severity composition by control domain.

4.1 Severity Distribution Observations

- **9%** of storage configuration findings were classified as critical severity, the highest critical severity share among the five domains illustrated, frequently associated with publicly accessible storage resources lacking appropriate access restriction.
- **8%** of identity and access management findings were classified as critical severity, commonly associated with excessive privilege assignment or absent multi factor authentication enforcement.
- **15%** of storage configuration findings were classified as high severity, the highest high severity share among the five domains.
- **34%** of compute hardening findings were classified as low severity, the highest low severity share among the five domains, suggesting a larger volume of minor configuration deviations relative to significant exposures in this domain.

4.2 Most Frequently Cited Specific Findings

- **Finding pattern 1:** Publicly accessible cloud storage resources lacking appropriate access restriction, consistently among the most frequently cited critical findings across audits reviewed in the period through 2021.
- **Finding pattern 2:** Absent or inconsistently enforced multi factor authentication for privileged accounts, a persistent high severity finding across identity and access management audits.
- **Finding pattern 3:** Insufficient log retention duration relative to applicable state or federal requirements, a common logging and monitoring finding contributing to the lower conformance observed in Section 3.1.
- **Finding pattern 4:** Unencrypted data at rest in storage resources not covered by default encryption policies, a recurring data protection finding, particularly in environments with resources provisioned before encryption by default became standard practice.

05 | Remediation Timelines and Bottlenecks

The time required to remediate audit findings varies considerably, with a meaningful share of findings remaining open well beyond the initial audit reporting period.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

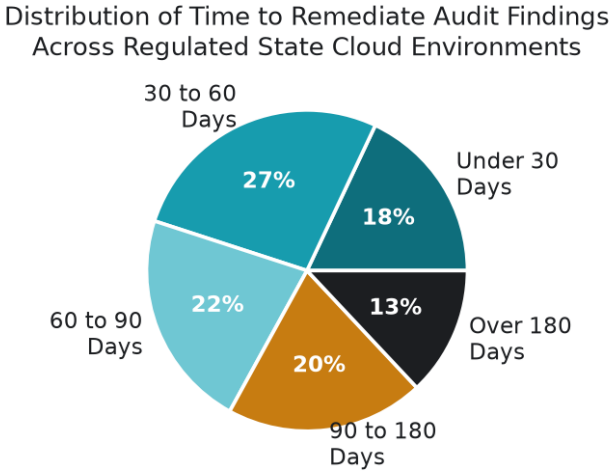

Figure 3. Distribution of time to remediate audit findings across regulated state cloud environments.

5.1 Remediation Timing Observations

- **18%** of findings were remediated in under 30 days, generally corresponding to lower complexity configuration changes such as adjusting a specific access control setting.
- **27%** of findings were remediated within 30 to 60 days, the largest single band, typically involving changes requiring change management review or limited testing.
- **22%** of findings required 60 to 90 days, often associated with changes affecting multiple dependent systems or requiring coordination across teams.
- **20%** of findings required 90 to 180 days, frequently tied to legacy system constraints or the need for budget approval to remediate.
- **13%** of findings remained open beyond 180 days, a share with direct implications for sustained audit risk given that these findings persist across multiple reporting cycles.

5.2 Common Remediation Bottlenecks

- **Bottleneck 1:** Legacy systems or resources provisioned before current benchmark versions were adopted frequently require more substantial remediation effort than newly provisioned resources.
- **Bottleneck 2:** Findings requiring budget approval for remediation, particularly where new tooling or licensing is required, extend timelines beyond what technical remediation alone would require.
- **Bottleneck 3:** Findings affecting shared infrastructure used by multiple applications or programs require cross team coordination that extends remediation timelines relative to single application findings.

06 | The Continuous Compliance Monitoring Approach

Continuous compliance monitoring, the practice of automatically and repeatedly assessing conformance against CIS Benchmark criteria rather than relying solely on periodic manual audit, represents a meaningful shift in how leading agencies approach audit readiness.

6.1 Core Elements of Continuous Monitoring

- **Automated scanning:** Automated scanning tools assess cloud resource configuration against CIS Benchmark criteria on a recurring, typically daily or more frequent, basis rather than only during formal audit windows.
- **Real time finding tracking:** New findings generated by continuous scanning are tracked and routed through a defined remediation workflow immediately upon detection, rather than accumulating until the next audit cycle.
- **Trend visualization:** Conformance trends are visualized over time, allowing security and compliance teams to identify degrading conformance before it accumulates into a significant audit exposure.

6.2 Reported Benefits of Continuous Monitoring

- **Faster detection:** agencies operating continuous monitoring reported detecting configuration drift and new findings substantially sooner than agencies relying on periodic manual assessment alone.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- **Shorter remediation timelines:** findings detected through continuous monitoring were reported to be remediated meaningfully faster than findings first identified during a periodic audit, reflecting the value of earlier detection.
- **Reduced audit surprise:** agencies with mature continuous monitoring reported fewer unexpected critical findings during formal audit cycles, since most findings had already been detected and were in active remediation before the formal audit began.

IMPLEMENTATION NOTE
Continuous monitoring does not eliminate the need for periodic formal audit, but it substantially changes the nature of that audit from a discovery exercise to a verification exercise, confirming that known findings are being managed appropriately rather than surfacing entirely new issues.

07 | The Five Stage Compliance Maturity Model

Agencies can be classified into one of five maturity stages describing their overall CIS benchmark compliance and audit readiness posture.

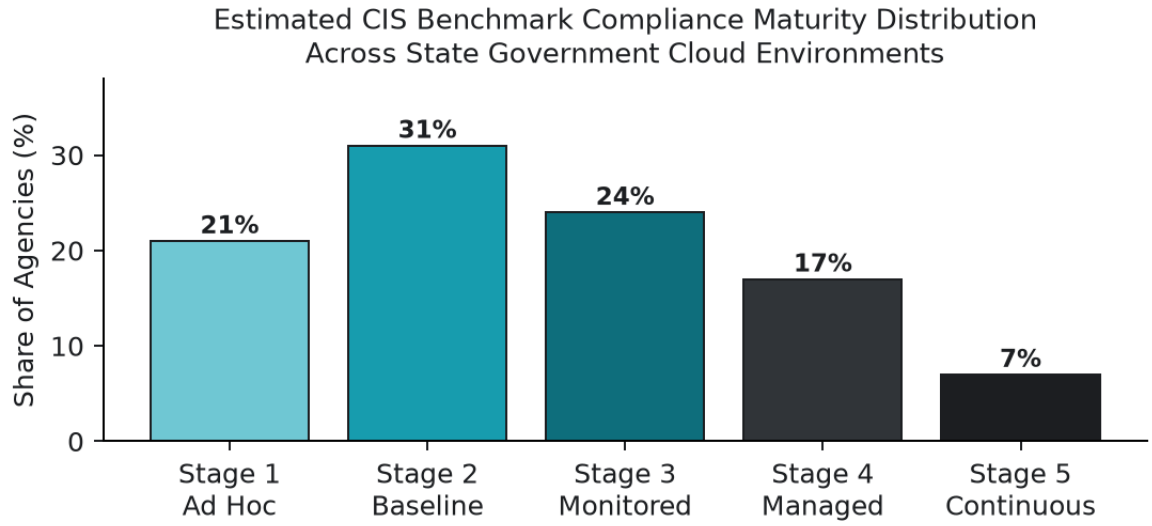

Figure 4. Estimated CIS benchmark compliance maturity distribution across state government cloud environments.

7.1 Stage Definitions

- **Stage 1: Ad Hoc:** No formal benchmark reference is applied; configuration decisions are made without systematic reference to CIS or comparable standards.
- **Stage 2: Baseline:** A baseline CIS benchmark scan has been conducted, but findings are addressed reactively without a structured remediation program.
- **Stage 3: Monitored:** Periodic, scheduled scanning occurs and findings are tracked, but scanning is not continuous and remediation timelines vary widely.
- **Stage 4: Managed:** Continuous monitoring, as described in Section 6, operates with defined remediation workflows and consistent timelines across most control categories.
- **Stage 5: Continuous:** Compliance posture is actively used to inform broader risk management decisions, with predictive identification of emerging conformance gaps before they become findings.

7.2 Estimated Distribution Observations

- **21%** of agencies examined were estimated to fall into Stage 1, Ad Hoc, reflecting environments where benchmark based configuration standards had not yet been systematically applied.
- **31%** were estimated to fall into Stage 2, Baseline, the largest single stage, representing agencies that had conducted an initial benchmark assessment without a sustained remediation program.
- **24%** were estimated to fall into Stage 3, Monitored, reflecting periodic but not continuous scanning practice.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- **17%** were estimated to fall into Stage 4, Managed, with continuous monitoring and defined remediation workflows in place.
- **7%** were estimated to fall into Stage 5, Continuous, the most mature classification observed.

08 | The Audit Readiness Lifecycle

Sustained audit readiness follows a recurring lifecycle rather than a linear, one time project, reflecting the continuous nature of cloud configuration change.

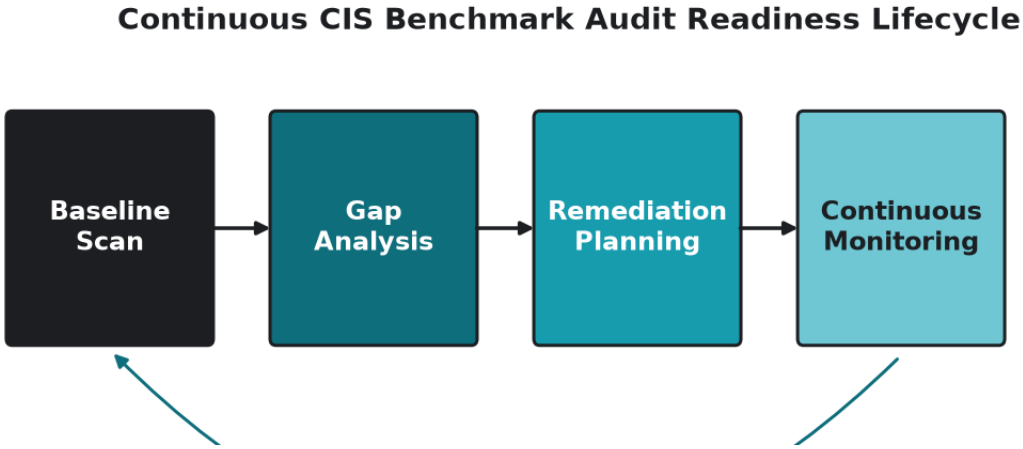

Figure 5. Continuous CIS benchmark audit readiness lifecycle, cycling from baseline scan through continuous monitoring and back.

8.1 Lifecycle Stage Descriptions

- **Baseline scan:** An initial or recurring scan establishes current conformance status against the applicable CIS Benchmark profile.
- **Gap analysis:** Scan results are analyzed to identify specific gaps, prioritized by severity and by the control category patterns described in Section 3.
- **Remediation planning:** Prioritized findings are assigned owners, remediation approaches, and target timelines, informed by the remediation bottleneck patterns described in Section 5.2.
- **Continuous monitoring:** Ongoing scanning, as described in Section 6, detects new findings and configuration drift, feeding back into the next gap analysis cycle.

8.2 Why the Lifecycle Model Matters for Audit Readiness

Agencies that treat CIS benchmark compliance as a single, discrete project rather than a recurring lifecycle frequently experience conformance degradation between the initial assessment and any subsequent formal audit, as new cloud resources are provisioned without the same rigor applied during the original assessment. The lifecycle model, particularly its continuous monitoring stage, is designed specifically to prevent this degradation.

09 | Governance and Ownership Structures

Sustained CIS benchmark compliance requires clear governance ownership spanning security, cloud operations, and, where relevant, individual program application teams.

9.1 Common Governance Roles

- **Security or compliance team:** Typically owns the CIS benchmark scanning program, sets the applicable conformance level and scope, and tracks aggregate conformance trends across the environment.
- **Cloud operations team:** Typically owns remediation of infrastructure level findings, such as network configuration or storage access settings.
- **Application or program team:** Typically owns remediation of application specific findings, such as application level access control configuration.
- **Agency leadership:** Typically reviews aggregate compliance posture and remediation progress at a governance cadence appropriate to the agency's risk tolerance and audit calendar.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

9.2 Common Governance Gaps

- Ownership for specific finding categories is often left ambiguous between cloud operations and application teams, particularly for findings affecting shared infrastructure.
- Aggregate compliance reporting to agency leadership is frequently ad hoc rather than scheduled, reducing leadership visibility into compliance trends between formal audit cycles.
- Remediation prioritization is sometimes driven primarily by ease of implementation rather than by the severity distribution patterns described in Section 4.1, resulting in lower severity findings being resolved ahead of higher severity findings.

9.3 Modernization Priorities

- **Priority 1:** Assign explicit ownership for each control category and finding type before continuous monitoring is implemented, avoiding ambiguity once finding volume increases.
- **Priority 2:** Establish a scheduled leadership reporting cadence using the aggregate metrics described in Section 14, rather than relying on audit season reporting alone.
- **Priority 3:** Prioritize remediation based on severity and category risk patterns rather than implementation ease alone.

10 | Cross Framework Alignment Considerations

CIS Benchmarks rarely operate in isolation; most regulated state government environments must also satisfy requirements under NIST 800-53, state specific security policy, and, for health and human services programs, federal program specific security requirements.

10.1 Alignment Observations

- **Observation 1:** CIS Benchmark controls map closely to a substantial portion of NIST 800-53 control families, particularly within access control, audit and accountability, and system and communications protection families, allowing agencies to use CIS scanning results as partial evidence toward broader NIST aligned compliance programs.
- **Observation 2:** State specific security policy frequently references CIS Benchmarks directly or incorporates equivalent configuration requirements, reducing the practical distinction between CIS conformance and state policy conformance in many cases.
- **Observation 3:** Federal program specific requirements, such as those applicable to health and human services or criminal justice information systems, sometimes impose additional or more stringent requirements beyond baseline CIS Benchmark criteria, requiring agencies to layer program specific controls on top of a CIS baseline.

ALIGNMENT NOTE
Agencies subject to multiple compliance frameworks benefit from mapping CIS Benchmark controls to each applicable framework once, centrally, rather than repeating that mapping exercise separately within each program area, reducing duplicate compliance effort.

11 | Risk Assessment and Mitigation Planning

CIS benchmark compliance programs carry execution risks that agencies should evaluate and mitigate deliberately, particularly given the audit consequences of unresolved findings.

11.1 Principal Risks

- **Risk 1: Storage exposure persistence.** Storage configuration findings carry the highest critical severity share observed in Section 4.1, and delayed remediation of these findings represents the most direct path to significant data exposure.
- **Risk 2: Logging and monitoring blind spots.** Given the lower conformance observed for logging and monitoring controls in Section 3.1, agencies may be unable to detect or investigate security incidents even where other controls are functioning correctly.
- **Risk 3: Chronic finding persistence.** Findings remaining open beyond 180 days, representing a meaningful share of all findings per Section 5.1, persist across multiple audit cycles and compound reputational and regulatory risk.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- **Risk 4: Governance ownership gaps.** Without the governance clarity described in Section 9, remediation ownership ambiguity can silently extend timelines for shared infrastructure findings.

11.2 Mitigation Approaches

- **Mitigation 1:** Prioritize storage configuration and identity and access management findings for accelerated remediation given their outsized critical severity representation.
- **Mitigation 2:** Invest specifically in logging and monitoring conformance improvement, given its role as a foundational detection capability underlying all other controls.
- **Mitigation 3:** Establish explicit service level expectations for remediation timelines by severity, with escalation triggered for findings approaching the 90 and 180 day thresholds identified in Section 5.1.
- **Mitigation 4:** Resolve governance ownership ambiguity before finding volume scales with continuous monitoring adoption.

12 | Implementation Roadmap

Translating this framework into an executable program requires sequencing baseline assessment, governance formation, remediation, and transition to continuous monitoring.

12.1 Roadmap Phases

- **Months 1 to 2, Baseline Assessment:** Conduct an initial CIS benchmark scan across the environment; establish the baseline conformance findings illustrated in Section 3.
- **Months 2 to 4, Governance and Prioritization:** Assign governance ownership per Section 9; prioritize findings by severity per Section 4.1 and category risk.
- **Months 3 to 9, Initial Remediation:** Address highest severity findings first, targeting the remediation timeline benchmarks described in Section 5.1.
- **Months 6 to 10, Continuous Monitoring Transition:** Implement automated, recurring scanning and real time finding tracking as described in Section 6.
- **Months 10 onward, Sustained Operations:** Operate the recurring audit readiness lifecycle described in Section 8 on an ongoing basis.

12.2 Governance Cadence Reference

- **Weekly during active remediation:** Review new findings and remediation progress against severity based service level expectations.
- **Monthly:** Review aggregate conformance trends and category level patterns with agency leadership.
- **Annually:** Conduct a full maturity stage reassessment using the model described in Section 7.

13 | Case Patterns and Industry Benchmarks

This article synthesizes recurring patterns observed across published cloud security research and public sector audit guidance through late 2021, rather than reporting on a single named agency.

13.1 Recurring Patterns

- **Pattern 1:** Agencies that implemented continuous monitoring prior to a formal audit reported fewer critical findings surfaced during that audit compared to agencies without continuous monitoring in place.
- **Pattern 2:** Agencies that mapped CIS Benchmark controls to NIST 800-53 once, centrally, reported reduced duplicate compliance effort across programs subject to multiple frameworks.
- **Pattern 3:** Agencies that prioritized remediation by severity, rather than by implementation ease, reported faster reduction in aggregate critical and high severity finding counts over successive quarters.
- **Pattern 4:** Agencies with clearly assigned governance ownership for shared infrastructure findings reported shorter remediation timelines for those findings compared to agencies with ambiguous ownership.

13.2 Observations Specific to Regulated Program Areas

- **Observation 1:** Health and human services and criminal justice information systems, subject to additional federal program specific security requirements layered on top of a CIS baseline, reported longer average remediation timelines than general purpose administrative systems, consistent with the added coordination complexity described in Section 10.1.
- **Observation 2:** Agencies serving multiple regulated program areas on shared cloud infrastructure benefited from a single, centralized compliance governance function rather than duplicating governance separately per program.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

14 | Key Performance Indicators for Ongoing Governance

Sustaining CIS benchmark compliance and audit readiness requires an ongoing measurement framework spanning conformance, finding severity, and remediation performance.

14.1 Recommended KPIs

- **Aggregate conformance rate:** The percentage of applicable CIS Benchmark controls in a conforming state, tracked overall and by control category, benchmarked against the category level figures presented in Section 3.1.
- **Open finding count by severity:** The count and share of open findings by severity level, tracked over time to confirm downward trend in critical and high severity findings specifically.
- **Mean time to remediate:** Average and median time to remediate findings by severity level, benchmarked against the distribution presented in Section 5.1.
- **Chronic finding rate:** The percentage of findings still open beyond 180 days, tracked as a specific indicator of chronic finding persistence risk described in Section 11.1.
- **Scanning coverage rate:** The percentage of cloud resources actively covered by continuous scanning, confirming that scanning coverage keeps pace with environment growth.
- **Maturity stage progression:** A composite score reflecting current classification against the five stage model in Section 7, tracked over successive annual reassessments.

GOVERNANCE REMINDER

KPIs should be reviewed on the weekly, monthly, and annual cadence described in Section 12.2, with particular attention to whether critical and high severity finding counts are trending downward and whether chronic finding rates are declining over successive review periods.

15 | Conclusion and Recommendations

CIS Benchmark compliance and audit readiness in regulated state government cloud environments benefits from treating compliance as a continuous, governed operational practice rather than a periodic, point in time audit preparation exercise. Agencies that adopt continuous monitoring, clear governance ownership, and severity informed remediation prioritization consistently report stronger conformance and shorter remediation timelines than agencies relying on periodic manual assessment alone.

15.1 Summary of Key Findings

- Logging and monitoring controls show the lowest average conformance among the categories examined, representing a foundational detection capability gap with implications for all other control categories.
- Storage configuration findings carry the highest critical severity representation, warranting prioritized remediation attention.
- A meaningful share of findings remain open beyond 180 days, representing sustained audit risk across multiple reporting cycles.
- Continuous monitoring is associated with faster detection, shorter remediation timelines, and fewer audit surprises compared to periodic manual assessment alone.

15.2 Recommendations

- **Recommendation 1:** Prioritize logging and monitoring control conformance improvement given its foundational role underlying detection capability across all other control categories.
- **Recommendation 2:** Implement continuous, automated scanning and real time finding tracking rather than relying on periodic manual audit as the primary compliance mechanism.
- **Recommendation 3:** Establish clear governance ownership for each control category and finding type before continuous monitoring adoption increases finding volume.
- **Recommendation 4:** Map CIS Benchmark controls to other applicable frameworks, including NIST 800-53 and state specific policy, centrally and once, to reduce duplicate compliance effort across program areas.

15.3 Closing Note

Agencies that build CIS benchmark compliance into ongoing operational practice, supported by continuous monitoring, clear governance, and severity informed prioritization, are positioned to sustain audit readiness between formal review cycles rather than treating each audit as an isolated, high effort discovery exercise.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

References

1) Center for Internet Security (CIS). (2021). *CIS benchmarks for cloud providers*. CIS Publication Series.
2) Center for Internet Security (CIS). (2021). *CIS controls* (Version 8). CIS Publication.
3) National Institute of Standards and Technology (NIST). (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Rev. 5).
4) National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1).
5) U.S. Government Accountability Office. (2021). *Cloud computing: Agencies have increased usage and realized benefits, but face challenges*. GAO Report.
6) U.S. Government Accountability Office. (2019). *Information security: Federal agencies need to address aging legacy systems* (GAO-19-471).
7) National Association of State Chief Information Officers (NASCIO). (2021). *State CIO top ten policy and technology priorities*. NASCIO Research Brief.
8) National Association of State Chief Information Officers (NASCIO). (2020). *State IT security governance and cloud compliance practices*. NASCIO Research Brief.
9) Cloud Security Alliance (CSA). (2020). *Cloud controls matrix* (Version 4). CSA Publication.
10) Cloud Security Alliance (CSA). (2019). *Security guidance for critical areas of focus in cloud computing* (Version 4.0). CSA Publication.
11) Center for Digital Government. (2021). *State government cloud security posture management practices*. Center for Digital Government Research Report.
12) Amazon Web Services. (2020). *AWS Well-Architected Framework: Security pillar*. AWS Whitepaper.
13) Microsoft Azure. (2021). *Azure Security Benchmark* (Version 3). Microsoft Technical Documentation.
14) Google Cloud. (2020). *Google Cloud security foundations guide*. Google Cloud Whitepaper.
15) Deloitte. (2020). *State government cybersecurity study: Cloud adoption and compliance*. Deloitte and NASCIO Joint Publication.
16) Government Technology. (2021). *States turn to continuous monitoring to close cloud compliance gaps*. e.Republic Government Technology Publication.
17) SANS Institute. (2020). *Critical security controls for effective cyber defense*. SANS Whitepaper.
18) American Institute of CPAs (AICPA). (2020). *SOC 2 trust services criteria and cross-framework mapping considerations*. AICPA Guidance.

