Guidehouse

# 2024 Section 912 Results and Considerations for 2025

Emma Sabio
Joshua Griste

outwit complexity™

# Agenda

- Introduction and Logistics
- 2024 Section 912 Overall Summary
- 2024 Section 912 Review Break Out
- 2025 Section 912 Considerations
- Q&A

# 2024 Section 912 Overall Summary

# Overview

Testing was aligned with the updated MAC ARS 5.1 and BPSSM rev 15 requirements across MACs.

9 Sections Reviewed:

| | | | |
|---|---|---|---|
| I | Risk Assessments | VI | Remedial activities, processes and reporting for deficiencies |
| II | Policies and procedures to reduce risk | VII | Incident detection, reporting and response |
| III | Systems security plans | VIII | Policies and procedures for continuity of operations and related physical security safeguards for IT |
| IV | Security awareness training | IX | Privacy Controls Testing |
| V | Periodic testing and evaluation of the effectiveness of IT security policies | | |

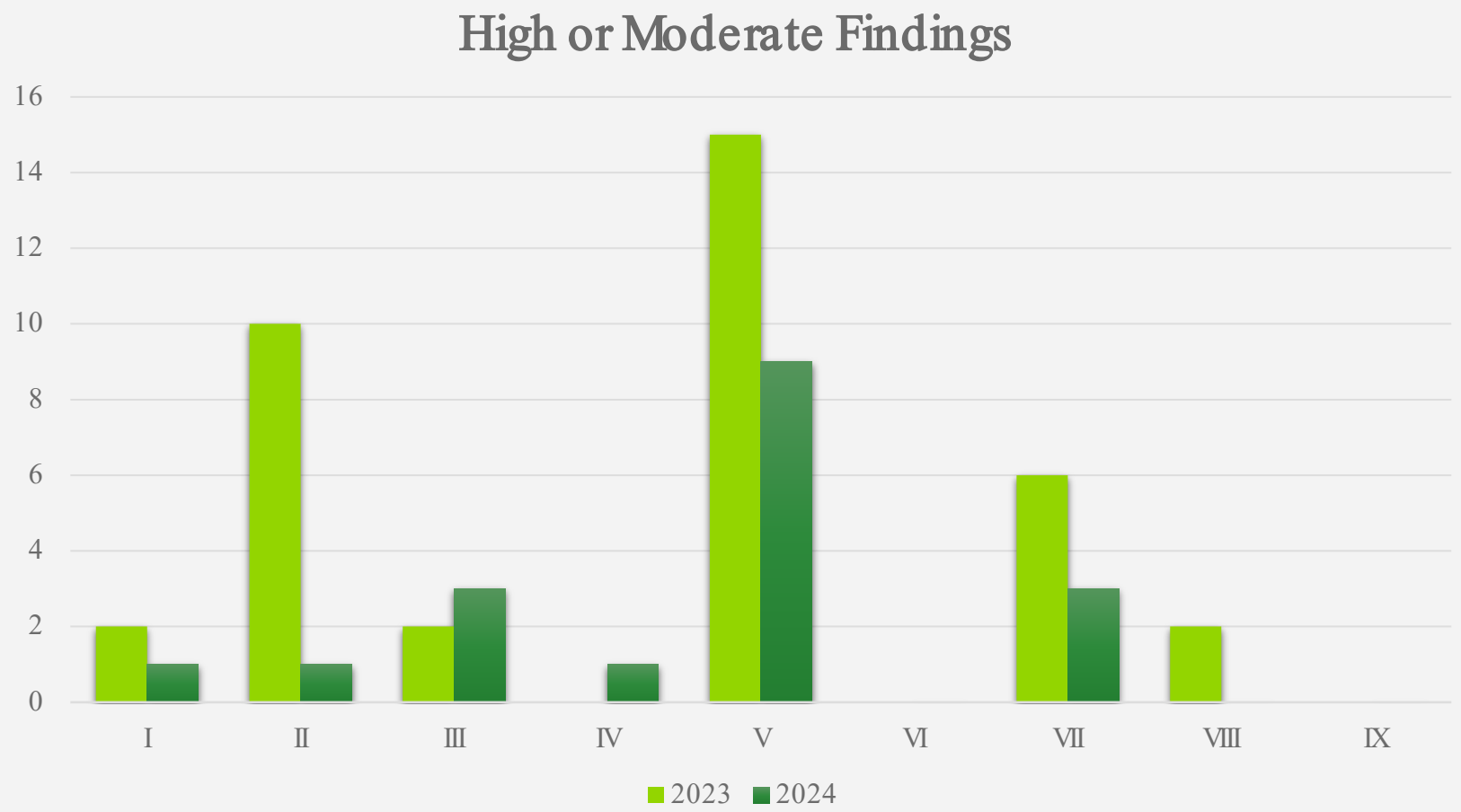
Guidehouse reviewed 7 Medicare Administrative Contractors (MACs) over a 4-week period from June to November 2024.

Activities performed outside the scope of the 912 Review:

- HVA Assessments
- Winter/Spring Oversights
- Winter Training Series
- Firewall Rule Config Review
- TDL Review
- Coming Soon – Authenticated Portal Testing

# Year-to-Year Comparison

The graph below represents the number of High or Moderate risk findings for each testing area during the 2023 and 2024 CMS Section 912 Reviews.



# 2024 Results by Testing Area

| Color | Description |
|---|---|
| Green(G) | No high-risk findings and two or less moderate risk findings. |
| Orange(O) | One high risk finding, or no high-risk findings and three or more moderate risk findings. |
| Red(R) | Two or more high risk findings. |

| I | II | III | IV | V | VI | VII | VIII | IX |
|---|---|---|---|---|---|---|---|---|
| G | G | G | G | G | G | G | G | G |
| G | G | G | G | O | G | G | G | G |
| G | G | G | G | G | G | G | G | G |
| O | G | G | G | O | G | G | G | G |
| G | G | G | G | G | G | G | G | G |
| G | G | G | G | O | G | G | G | G |
| G | G | G | G | G | G | G | G | G |

# Top Findings Issued

| Control Activity | Overall Finding | Number of Contractors Affected |
|---|---|---|
| V.E | Security weaknesses were identified as part of the external network penetration test. | 5 |
| VII.D | Log review processes did not comply with CMS requirements. | 3 |
| V.F | System component inventory processes were not implemented in accordance with CMS requirements. | 2 |
| III.C | Processes for annual recertification of portal accounts were not in accordance with CMS requirements. | 2 |

# 2024 Section 912 Review Break Out

# Section I. Risk Assessments

## Suggestions To Reduce Risk

- Verify that vulnerability remediation efforts are fully implemented in accordance with CMS requirements and include the formal tracking of vulnerabilities.
- Review Interconnection Security Agreements on an ongoing basis and ensure there are ISAs for each external service provider.

# Section II. Policies and Procedures to Reduce Risk

## Suggestions To Reduce Risk

- Update and verify Security Configuration Checklists (SCCs) are based on the most recent security guidance and compliant with CMS requirements.
- Verify that anti-virus configurations and timing of scans are set in accordance with CMS requirements.
- Have a formalized process for periodic exfiltration testing.
- Confirm that malicious software protection mechanisms are installed, are current, and are operating effectively for systems within the environment.
- Verify that whitelisting software is installed in accordance with CMS requirements.

# Section III. System Security Plans

## Suggestions To Reduce Risk

- Develop processes to perform security due diligence on each Cloud Service Provider (CSP) implementation and maintain complete and accurate documentation.
- Develop Responsibility Line Matrices (RLMs) for all of the CSPs within the environment.
- Review CSP Service Level Agreements on an annual basis.
- Implement a formalized process for monitoring the risks and impacts of each CSP in the environment.
- Update the SSP regularly to make certain it reflects the current operating environment.
- Ensure access control policies and procedures are enforced in accordance with CMS BPSSM requirements.

**Notable Achievements**
Improved SSP documentation and cloud control implementation.

# Section IV. Security Awareness Training

## Suggestions for Continued Success

- Update and maintain the Rules of Behavior, Security Awareness Training, and Privacy Training in accordance with CMS requirements.
- Ensure completion and tracking of new hire and annual refresher of Security Awareness and Privacy Training.

# Section V. Periodic and Evaluation of the Effectiveness of IT Security Policies

## Suggestions To Reduce Risk

- Enhance processes and provide documentation within TDL230494 submission.
- Remediate and/or track failed configurations checks for all platforms.
- Document deviations, exceptions, and technical limitation acknowledgement where applicable.
- Develop and implement corrective action plans to address identified security weaknesses.
- Enforce change management procedures to ensure controlled and secure system modifications.
- Maintain a system component inventory that is a complete and accurate listing of systems and devices within their environment.

**Notable Achievements**
Improved performance in TDL documentation, and accurate diagnostic configurations.

# Section VI. Remedial Activities, Processes, and Reporting for Deficiencies

## Suggestions for Continued Success

- Track and record security weaknesses identified within CFACTS in accordance with CMS requirements.

# Section VII. Incident Detection, Reporting, and Response

## Suggestions To Reduce Risk

- Ensure continued education and discussion of the log review process.
- Integrate solutions to effectively improve processes and technical capability around log review.
- Complete monthly manual review in accordance with CMS BPSSM requirements.

# Section VIII. Policies and Procedures for Continuity of Operations and Physical Security Safeguards

## Suggestions To Reduce Risk

- Confirm that weekly and daily incremental backups are being performed in accordance with CMS requirements.
- Implement media disposal processes in accordance with NIST800-88 requirements.
- Perform validations of media location accuracy.
- Report lost or missing assets in accordance with CMS requirements.

# Section IX. Privacy Controls Testing

## Suggestions for Continued Success

- Maintain an inventory listing of systems and applications that process or maintain PII in accordance with CMS requirements.

# 2025 Section 912 Considerations

Guidehouse

# Q&A