Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

REVIEW OF MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2021

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Amy J. Frontz
Deputy Inspector General
for Audit Services

July 2022
A-18-22-11300

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These audits help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief
Date: July 2022
Report No. A-18-22-11300

U.S. Department of Health & Human Services
Office of Inspector General

Review of Medicare Administrative Contractor Information Security Program Evaluations for Fiscal Year 2021

Why OIG Did This Audit

The Social Security Act requires each Medicare administrative contractor (MAC) to have its information security program evaluated annually by an independent entity. The Centers for Medicare & Medicaid Services (CMS) contracted with Guidehouse, LLP, to evaluate information security programs at the MACs, using a set of agreed-upon procedures (AUPs); HHS OIG must submit to Congress annual reports on the results of these evaluations and include assessments of their scope and sufficiency. This report fulfills that responsibility for fiscal year (FY) 2021.

Our objectives were to assess the scope and sufficiency of MAC information security program evaluations and report the results of those evaluations.

How OIG Did This Audit

We reviewed Guidehouse's working papers to determine whether Guidehouse sufficiently addressed all areas required by the AUPs. We also determined whether all security-related weaknesses were included in the Guidehouse reports by comparing supporting documentation with the reports. We determined whether all gaps in the Guidehouse reports were adequately supported by comparing the reports with the Guidehouse working papers.

What OIG Found

Guidehouse's evaluations of the contractor information security programs were adequate in scope and sufficiency. Guidehouse identified a total of 95 gaps at the 7 MACs in FY 2021, which was 4 percent less than the number of gaps for the same 7 MACs in FY 2020. The number of high- and moderate-risk gaps decreased by 39 percent from FY 2020. Deficiencies remained in eight of the nine Federal Information Security Modernization Act of 2014 control areas that were tested. The results warrant CMS continuing its oversight visits to ensure that the MACs remediate all gaps to improve the MACs' IT security, especially those with increased gaps from the previous year. Gaps that were similar to those from prior years should be considered repeat findings to highlight systemic problems and the existence of continued exposure to known weaknesses.

What OIG Recommends

This report contains no recommendations.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/182211300.asp.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Social Security Act (the Act), as modified by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) requires the Department of Health and Human Services, Office of Inspector General, to report to Congress the results of annual independent evaluations of the information security programs of Medicare administrative contractors (MACs). These evaluations must address the eight major requirements enumerated in the Federal Information Security Modernization Act of 2014 (FISMA). The Act also requires evaluations of the information security controls for a subset of systems but does not specify the criteria for these evaluations. This report fulfills that responsibility for fiscal year (FY) 2021.

OBJECTIVES

Our objectives were to assess the scope and sufficiency of MAC information security program evaluations and report the results of those evaluations.

BACKGROUND

The Medicare Program

The Centers for Medicare & Medicaid Services (CMS) administers Medicare. Medicare is a health insurance program for people age 65 or older, people under age 65 with certain disabilities, and people of all ages with end-stage renal disease. In FY 2021, Medicare paid approximately $733 billion on behalf of approximately 64 million Medicare beneficiaries. CMS contracts with MACs to administer Medicare benefits paid on a fee-for-service basis. In FY 2021, seven distinct entities served as MACs for Medicare Parts A and B to process and pay Medicare fee-for-service claims.

Medicare Prescription Drug, Improvement, and Modernization Act of 2003

The MMA added information security requirements for MACs to section 1874A of the Act. (See 42 U.S.C. § 1395kk-1.) Each MAC must have its information security program evaluated annually by an independent entity (the Act § 1874A(e)(2)(A)). This section requires that these evaluations address the eight major requirements enumerated in FISMA. (See 44 U.S.C. § 3544(b)). These requirements, referred to as “FISMA control areas” in this report, are:

1. periodic risk assessments;

2. policies and procedures to reduce risk;

3. system security plans;

4. security awareness training;

5. periodic testing of information security controls;

6. remedial actions;

7. incident detection, reporting, and response; and

8. continuity of operations for information technology (IT) systems.

CMS added a ninth area for testing starting in FY 2015:

9. privacy.

Section 1874A(e)(2)(A)(ii) of the Act requires that the effectiveness of information security controls be tested for an appropriate subset of MACs' information systems. However, this section does not specify the criteria for evaluating these security controls.

Additionally, section 1874A(e)(2)(C)(ii) of the Act requires us to submit to Congress annual reports on the results of such evaluations, including assessments of their scope and sufficiency.

CMS Evaluation Process for Fiscal Year 2021

CMS developed agreed-upon procedures (AUPs) for the program evaluation on the basis of the requirements of section 1874A(e)(1) of the Act, FISMA, information security policy and guidance from the Office of Management and Budget and the National Institute of Standards and Technology (NIST), and the Government Accountability Office's (GAO's) *Federal Information Systems Controls Audit Manual* (FISCAM). In FY 2021, the independent auditors, Guidehouse, LLP, under contract with CMS, used the AUPs to evaluate the information security programs at the seven entities that served as MACs. Two of the entities had multiple contracts with CMS to fulfill their responsibilities as Medicare Parts A and B MACs and durable medical equipment MACs. As a result, Guidehouse issued nine separate reports.

To comply with the section 1874A(e)(2)(A)(ii) requirement to test the effectiveness of information security controls for an appropriate subset of contractors' information systems, CMS included testing of Medicare claim processing systems hosted at the Medicare data centers. Medicare data centers are used for "front-end" preprocessing of claims received from providers and "back-end" issuing of payments to providers after claims have been adjudicated.

The results of the MAC information security program evaluations are presented in terms of gaps, which are defined as a MAC's incomplete implementation of FISMA or CMS core security requirements. Guidehouse categorized gaps into three categories: high, moderate, and low risk. The MACs are responsible for developing a corrective action plan for each high- and moderate-risk gap, and CMS is responsible for tracking all corrective action plans and ensuring that such gaps are remediated in a timely manner. CMS does not require corrective action plans for low-risk gaps involving a MAC's internal controls and operations, but those gaps are reviewed with the MACs during oversight visits.

CMS conducted a virtual oversight visit at each MAC during the year to address all gaps identified by Guidehouse during the prior year's reviews.

HOW WE CONDUCTED THIS AUDIT

We evaluated the FY 2021 results of the independent evaluations of the MACs' information security programs. We did not include an evaluation of internal controls.

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we did not obtain comments from Guidehouse. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A contains the details of our audit scope and methodology.

RESULTS OF AUDIT

Guidehouse's evaluations of the contractor information security programs were adequate in scope and sufficiency. At the 7 MACs evaluated in FY 2021, Guidehouse identified a total of 95 gaps, of which 6 were high-risk gaps, 19 were moderate-risk gaps, and 70 were low-risk gaps. The number of high- and moderate-risk gaps decreased by 39 percent from FY 2020.

ASSESSMENT OF SCOPE AND SUFFICIENCY

Guidehouse's evaluations of the MAC information security programs adequately encompassed in scope and sufficiency the nine control areas reviewed.

RESULTS OF EVALUATIONS ON MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAMS

As shown in Table 1 on the next page, Guidehouse identified a total of 95 gaps at the 7 MACs in FY 2021. The number of gaps by contractor ranged from 9 to 18 and averaged 14. See Appendix B for a list of gaps per FISMA control area by contractor.

Table 1: Range of Medicare Administrative Contractor Gaps, FYs 2020 and 2021

			Number of Contractors With:		
FY	Number of Contractors	Total Gaps	0–10 Gaps	11–15 Gaps	16+ Gaps
2020	7	99	0	6	1
2021	7	95	2	3	2

The total number of gaps reported for the 7 MACs that Guidehouse evaluated decreased by 4 percent in FY 2021 (from 99 in FY 2020 to 95 in FY 2021). There were 2 MACs with 10 or fewer gaps, the number of MACs with 11 to 15 gaps decreased by 3, and the number of MACs with 16 or more gaps increased by 1. Five MACs had fewer gaps in FY 2021, and two MACs had more gaps. See Appendix C for the FY 2020 to FY 2021 percentage change in gaps per MAC.

Table 2 summarizes the gaps found in each FISMA control area in FYs 2020 and 2021 and the number of contractors with one or more gaps. Gaps in five of the nine FISMA control areas tested in FY 2020 and FY 2021 decreased in FY 2021, with a decrease by one to three. Gaps in three of the nine FISMA control areas tested increased in FY 2021 by one or four. One of the nine FISMA control areas tested in FY 2020 and FY 2021 had no change in gaps.

Table 2: Gaps by Federal Information Security Modernization Act Control Area in FY 2021

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2020	FY 2021	FY 2020	FY 2021
Risk Assessments	2	6	2	5
Policies and Procedures to Reduce Risk	22	20	7	7
Systems Security Plans	14	12	7	5
Security Awareness Training	4	1	3	1
Periodic Testing and Evaluation of the Effectiveness of IT Security Policies	31	31	7	7
Remedial Activities, Processes and Reporting for Deficiencies	0	1	0	1
Incident Detection, Reporting, and Response	15	14	7	6
Continuity of Operations for IT Systems	9	10	5	6
Privacy Controls Testing	2	0	2	0
Total	**99**	**95**		

At the 7 MACs in FY 2021, Guidehouse identified a total of 95 gaps, of which 6 were high-risk gaps, 19 were moderate-risk gaps, and 70 were low-risk gaps. The number of high-risk gaps decreased by 50 percent (from 12 in FY 2020 to 6 in FY 2021), moderate-risk gaps decreased by 34 percent (from 29 in FY 2020 to 19 in FY 2021), and low-risk gaps increased by 21 percent (from 58 in FY 2020 to 70 in FY 2021). Guidehouse identified one repeat gap from FY 2020. In many instances, controls that were tested had similar findings from the previous year but were not considered repeat findings by Guidehouse because some of the gaps resulted from different systems being tested in the current year.

The MAC information security program evaluations covered several subcategories within each FISMA control area. Guidehouse assigned individual gaps an overall risk level on a subjective basis after considering the impact on CMS and likelihood of occurrence.

The following sections discuss the three FISMA control areas containing the most gaps. See Appendix D for descriptions of each subcategory tested for the three FISMA control areas.

Periodic Testing and Evaluation of the Effectiveness of IT Security Policies

The effectiveness of information security policies, procedures, practices, and controls should be tested and evaluated at least annually (NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Control CA-2). Security testing enables organizations to measure levels of compliance in areas such as patch management, password policy, and configuration management (NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, section 2.3). Changes to an application should be tested and approved before being put into production (FISCAM, section 3.3).

All seven MACs had from four to six gaps each related to periodic testing and evaluation of the effectiveness of information security policies. In total, Guidehouse identified 31 gaps in this area. Following are examples of these gaps:

- System component inventory processes were not implemented in accordance with CMS requirements.

- System security configurations did not comply with CMS requirements.

- Wireless access monitoring was not performed in accordance with CMS requirements.

Without an adequate system inventory process for all systems and devices and a comprehensive program for periodically testing, monitoring, and ensuring that information security controls are operating as required, management has no assurance that appropriate safeguards are in place to mitigate identified risks.

Policies and Procedures To Reduce Risk

According to NIST SP 800-53, Chapter 2.1:

> The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program for the management of risk—that is, the risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation of information systems. Risk-based approaches to security control selection and specification consider effectiveness, efficiency, and constraints due to applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

All seven MACs had one to four gaps each related to policies and procedures to reduce risk. In total, Guidehouse identified 20 gaps in this area. Following are examples of these gaps:

- Systems operating in the contractors' environments did not have the latest patches installed.[1]
- Security configuration controls were not fully documented in accordance with CMS requirements.
- Mobile encryption requirements did not comply with CMS requirements.

Ineffective policies and procedures to reduce risk could jeopardize an organization's mission, information, and IT assets. Without adequate configuration standards and the latest security patches, systems could be exploited by known vulnerabilities that could lead to unauthorized disclosure of data, data modification, or data unavailability.

Incident Detection, Reporting, and Response

According to NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide:*

> Organizations should ensure that incident response policies and procedures and business continuity processes are in sync; and have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements, which relates to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support. An incident response capability is therefore necessary for rapidly detecting

[1] A patch is a piece of software designed to correct security and functionality problems in software programs and firmware.

incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

Six MACs had from one to three gaps each related to incident detection, reporting, and response. In total, Guidehouse identified 14 gaps in this area. Following are examples of these gaps:

- Incident reporting policies and procedures were not documented in accordance with *CMS Business Partner System Security Manual* requirements.

- Incident reporting was not performed in accordance with CMS requirements.

- Log review processes did not comply with CMS requirements.

Incident response is the first line of defense when responding to an attack, such as the Solar Winds attack. Effective incident response can minimize extensive damage to systems and networks. Without adequate and timely review of all audit logs that can identify potential security incidents, entities could experience slow and incomplete responses and negative business effects (e.g., extensive damage to computer systems, periods without computer service, and periods when data are unavailable).

OVERSIGHT REVIEWS

CMS performs at least one oversight review per year of each MAC to address gaps identified by Guidehouse. During FY 2021, CMS virtually visited each of the seven MACs and reviewed selected MAC controls and operations for cybersecurity, emphasizing configuration management, log monitoring, end-of-life software, firewall ruleset review results, and MAC-specific topics.

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the seven MACs reviewed by Guidehouse. The total number of gaps identified at the MACs had decreased from FY 2020. Deficiencies remained in eight of the nine FISMA control areas tested. The results warrant CMS continuing its oversight visits to ensure that the MACs remediate all gaps to improve the MACs' IT security, especially those with increased gaps from the previous year. Gaps that were similar to those from prior years should be considered repeat findings to highlight systemic problems and the existence of continued exposure to known weaknesses.

This report contains no recommendations.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2021 results of the independent evaluations of the MACs' information security programs. Our review did not include an evaluation of internal controls. We performed our reviews of Guidehouse working papers from March to June 2022.

METHODOLOGY

To accomplish our objectives, we performed the following steps:

- To assess the scope of the evaluations of contractor information security programs, we determined whether the AUPs included the eight FISMA control areas enumerated in section 1874A(e)(1) of the Act.

- To assess the sufficiency of the evaluations of contractor information security programs, we reviewed Guidehouse working papers supporting the evaluation reports to determine whether Guidehouse sufficiently addressed all areas required by the AUPs. We also determined whether all security-related weaknesses were included in the Guidehouse reports by comparing supporting documentation with the reports. We determined whether all gaps in the Guidehouse reports were adequately supported by comparing the reports with the Guidehouse working papers.

- To report on the results of the evaluations, we aggregated the results in the individual contractor evaluation reports. For the Guidehouse evaluations, we used the number of gaps listed in the individual MAC evaluation reports to aggregate the results.

We provided CMS with a draft audit report on July 13, 2022, for review. CMS had no written comments.

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we did not obtain comments from Guidehouse. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: GAPS BY FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 CONTROL AREA AND MEDICARE ADMINISTRATIVE CONTRACTOR IN FISCAL YEAR 2021

	Control Areas									
MAC	Risk Assessments	Policies and Procedures To Reduce Risk	Systems Security Plans	Security Awareness Training	Periodic Testing and Evaluation of the Effectiveness of IT Security Controls	Remedial Activities, Processes and Reporting for Deficiencies	Incident Detection, Reporting, and Response	Continuity of Operations for IT Systems	Privacy Controls Testing	Total Gaps
1	1	3	0	0	4	0	1	2	0	11
2	1	4	4	0	4	0	3	2	0	18
3	0	1	1	0	5	0	2	0	0	9
4	2	2	1	1	4	1	3	1	0	15
5	1	4	4	0	4	0	3	2	0	18
6	1	3	0	0	4	0	0	2	0	10
7	0	3	2	0	6	0	2	1	0	14
Total	**6**	**20**	**12**	**1**	**31**	**1**	**14**	**10**	**0**	**95**

APPENDIX C: CHANGE IN GAPS PER MEDICARE ADMINISTRATIVE CONTRACTOR, FISCAL YEARS 2020 AND 2021

MAC	FY 2020 Gaps	FY 2021 Gaps	# Change	% Change
1	12	11	(1)	(8)
2	15	18	3	20
3	12	9	(3)	(25)
4	19	15	(4)	(21)
5	14	18	4	29
6	12	10	(2)	(17)
7	15	14	(1)	(7)
Total	**99**	**95**	**(4)**	**(4%)**

APPENDIX D: RESULTS OF MEDICARE ADMINISTRATIVE CONTRACTOR EVALUATIONS FOR FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS

PERIODIC TESTING AND EVALUATION OF THE EFFECTIVENESS OF IT SECURITY CONTROLS

The evaluations of the MAC information security program covered nine subcategories related to the periodic testing and evaluation of the effectiveness of IT security controls. The evaluation reports identified a total of 31 gaps in this FISMA control area. (See Table 3.)

Table 3: Gaps in the Area of Periodic Testing and Evaluation of the Effectiveness of IT Security Policies in FY 2021

	Subcategory	**No. of Gaps in This Area**
1	Configuration management processes are performed in accordance with CMS requirements.	6
2	Change control management procedures exist.	0
3	Change control procedures are tested by management to make certain they are in use.	0
4	Systems are configured according to the contractor's documented security configuration checklists.	7
5	Weaknesses are identified by Guidehouse during a network attack and penetration test.	7
6	A formally maintained system component inventory is up to date and accurate.	6
7	The organization's Internet portal is compliant with section 508 of the Rehabilitation Act of 1973.	2
8	The organization has implemented email and web browser protections.	1
9	Wireless network access controls exist.	2
	Total	**31**

POLICIES AND PROCEDURES TO REDUCE RISK

The evaluations of the MAC information security program assessed 10 subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 20 gaps in this FISMA control area. (See Table 4.)

Table 4: Gaps in the Area of Policies and Procedures To Reduce Risk in FY 2021

	Subcategory	**No. of Gaps in This Area**
1	The system and network boundaries have been subjected to periodic reviews or audits. Management reports exist for review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews, and penetration assessments.	0
2	Results of management's compliance reviews with the CMS Acceptable Risk Safeguards.	0
3	Security policies and procedures include controls to address platform security configurations.	3
4	Security policies and procedures include controls to address patch management.	0
5	The latest patches have been installed on contractors' systems.	5
6	Security settings are included within checklists and comply with Defense Information Systems Agency standards.	7
7	Malicious software protection mechanisms have been installed on workstations and laptops, are up to date and operating effectively, and administrators are alerted of any malicious software identified on workstations and laptops.	3
8	Organization maintains an approved software whitelist and enforces the whitelist with both preventative and detective controls.	0
9	Organization employs full-device or container encryption to protect the confidentiality and integrity of information on approved mobile devices.	2
10	Organization implements data protection mechanisms that prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.	0
	Total	**20**

INCIDENT DETECTION, REPORTING, AND RESPONSE

The evaluations of the MAC information security program assessed six subcategories related to incident detection, reporting, and response. The evaluation reports identified a total of 14 gaps in this FISMA control area. (See Table 5.)

Table 5: Gaps in the Area of Incident Detection, Reporting, and Response in FY 2021

	Subcategory	**No. of Gaps in This Area**
1	Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.	2
2	Management has procedures to take and has taken action in response to unusual activity, intrusion attempts, and actual intrusions, including reporting.	2
3	Management incident response processes and procedures are documented in accordance with CMS requirements.	0
4	Log review policies and procedures for IT platforms that support contractor operations are documented in accordance with CMS requirements.	4
5	Log review results are evaluated for the completion of documented procedures.	5
6	Processes exist to analyze and correlate audit records across different repositories.	1
	Total	**14**