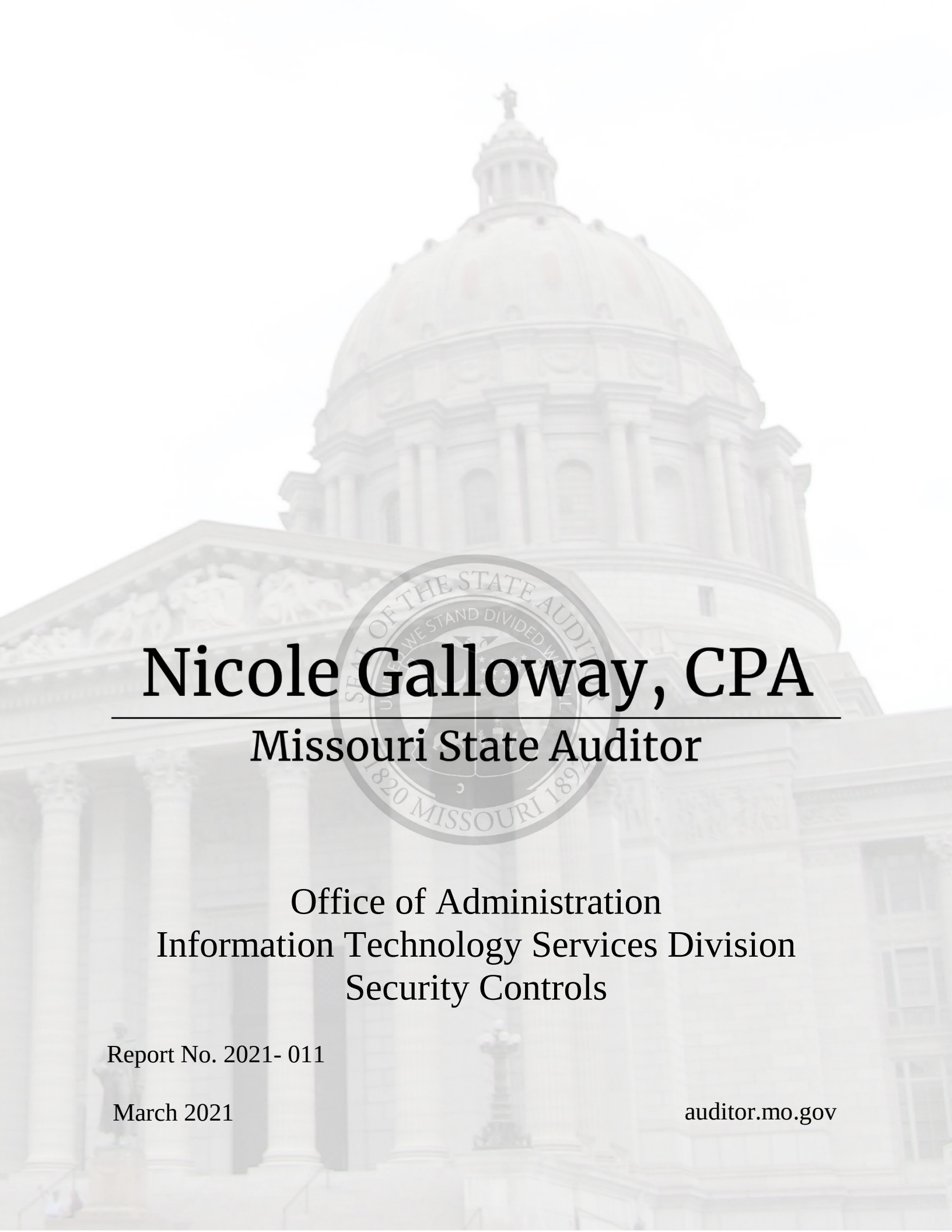


Nicole Galloway, CPA

Missouri State Auditor

Office of Administration
Information Technology Services Division
Security Controls

Report No. 2021- 011

March 2021

auditor.mo.gov

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of Office of Administration Information Technology Services Division Security Controls

Service Level Agreements	The Office of Administration Information Technology Services Division (ITSD) has not comprehensively developed or updated service level agreements between the ITSD and the state agency customers it serves.
Contingency Planning Policy	The ITSD has not formally adopted or documented an enterprise-wide contingency planning policy, including overall contingency objectives, an organizational framework, and comprehensive procedures.
Electronic Communication Policy	The ITSD has not developed records management and retention policies incompliance with the Missouri Secretary of State Records Services Division guidance, as approved by the Missouri State Records Commission.

In the areas audited, the overall performance of this entity was **Good**.*

*****The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

Excellent: The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.

Good: The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.

Fair: The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.

Poor: The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

Office of Administration
Information Technology Services Division Security Controls
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Michael L. Parson, Governor
and
Sarah H. Steelman, Commissioner
Office of Administration
Jefferson City, Missouri

We have audited certain internal controls, including security controls, designed to protect data and information maintained by the Office of Administration - Information Technology Services Division. This audit was conducted in fulfillment of our duties under Chapter 29, RSMo. The objectives of our audit were to:

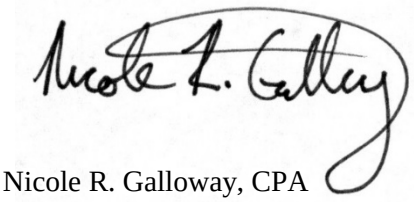
1. Evaluate internal controls over significant management and financial functions.

2. Evaluate compliance with certain legal provisions.

3. Evaluate the economy and efficiency of certain management practices and information system control activities.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our 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 such a basis.

For the areas audited, we identified (1) deficiencies in internal controls, (2) no significant noncompliance with legal provisions, and (3) the need for improvement in management practices and information system control activities. The accompanying Management Advisory Report presents our findings arising from our audit of the Office of Administration - Information Technology Services Division.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Director of Audits:	Jon Halwes, CPA, CGFM
Audit Manager:	Alex R. Prenger, M.S.Acct., CPA, CISA, CFE, CGAP
In-Charge Auditor:	Patrick M. Pullins, M.Acct., CISA, CFE
Audit Staff:	Zachery L. Harris

Office of Administration
Information Technology Services Division Security Controls
Introduction

Background

The Information Technology Services Division (ITSD) is a division of the Office of Administration (OA). The ITSD was formed in January 2005 to consolidate information technology (IT) staff and funding for executive branch agencies.

The ITSD is responsible for coordinating and providing IT services to executive branch agencies. Services provided by the division include the operation of the State Data Center to provide a centralized computer facility used by state agencies and elected officials; operation of the state telecommunications network; desktop support; web, mainframe, and other communication platform and application development and maintenance; data management and database support; email services; help desk services; cyber security; and an IT education center for state employees.

The ITSD directly supports the following executive offices and state agencies: Agriculture, Commerce and Insurance,[1] Corrections, Economic Development, Elementary and Secondary Education, Governor's Office, Health and Senior Services, Higher Education and Workforce Development, Labor and Industrial Relations, Lieutenant Governor's Office, Mental Health, Natural Resources, Office of Administration, Public Safety,[2] Revenue,[3] and Social Services.

Michael Cheles served as Chief Information Officer from October 2018 to December 2019. Jeffrey Wann was appointed Chief Information Officer in January 2020. At June 30, 2020, the division had 919 employees.

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information.

Scope and Methodology

The scope of our audit included (1) internal controls established and managed by the ITSD, (2) policies and procedures, and (3) other management functions and compliance issues in place during the year ended June 30, 2020.

[1] Department of Commerce and Insurance except for Public Service Commission.

[2] Department of Public Safety except for Missouri National Guard, Missouri State Highway Patrol, and Missouri Gaming Commission.

[3] Department of Revenue except for Lottery Commission.

Our methodology included reviewing written policies and procedures, and interviewing various ITSD personnel. We obtained an understanding of internal control that is significant to the audit objectives and assessed the design and implementation of such internal control to the extent necessary to address our audit objectives. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

To evaluate the satisfaction of state agencies with the services provided by the ITSD, we surveyed 32 officials of 19 consolidated agencies (or divisions of agencies as applicable). Officials were also invited to forward the survey to other staff of their agency who could provide pertinent information. We received 25 responses. Respondents were given the option to remain anonymous, so it is unknown if all agencies/divisions provided responses. Responses are summarized in the Appendix.

We based our evaluation on accepted state, federal, and international standards and best practices related to information technology security controls from the following sources:

- Missouri Adaptive Enterprise Architecture (MAEA)
- National Institute of Standards and Technology (NIST)
- ISACA

Officials from the OA did not provide certain written representations to our office as requested. It is standard practice of the State Auditor's Office to require such representations, as allowed by Government Auditing Standards, to help ensure sufficient, appropriate evidence has been obtained. Historically, state agencies have not refused to provide such assurances.

We asked OA officials to provide, among other things, the following written representations:

- "We have not knowingly withheld from you any records that in our judgment would be relevant to your audit."

- "We are responsible for the division's compliance with provisions of laws, regulations, contracts, and grant agreements applicable to it; and we have identified, and disclosed to you, all such provisions that we believe have a significant effect on operations. We have complied with all aspects of laws, regulations, contracts, and grant agreements that would have a significant effect on operations in the event of noncompliance."

OA officials did not provide these written representations and instead provided the following representations, which significantly altered the meaning of these representations:

- "We have not knowingly withheld from you any records you requested that in our judgment would be relevant to your review."

- "We are responsible for the division's compliance with the Revised Statutes of Missouri, state regulations, and contracts as they relate to security controls and, within the limits of our authority, have performed activities to comply with the same. We have not identified any grant agreements to which ITSD is a party related to security controls."

In effect, OA officials declined to provide assurance they (1) had not withheld relevant information from audit staff and (2) had disclosed all provisions of laws, regulations, contracts, and grant agreements that the agency believed would have a significant effect on the audit.

Refusal to provide such representations is concerning and may indicate information potentially relevant to our audit was knowingly withheld from us by OA officials.

1. Service Level Agreements

The Office of Administration (OA) Information Technology Services Division (ITSD) has not comprehensively developed or updated service level agreements between the ITSD and the state agency customers it serves.

A service level agreement (SLA) is a document used by organizations entering into a partnership for the provision of information technology (IT) services. According to ISACA, an SLA is used to align IT enabled products and services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT products and services. SLAs can be in-house between an organizational unit and its IT department, external between an entity and an outside service provider, or internal within the units of a service provider.[4]

While the ITSD provided an example of a current SLA in place between the division and a consolidated agency, the agreement is not comprehensive, and does not document the specific responsibilities and obligations of the agency or the ITSD. For example, the document did not discuss the specific systems to be covered by the agreement, responsibilities for governance or decision making regarding the systems, and reporting obligations of the parties. In addition, while the SLA, which was not dated but appeared to be from approximately 2005, was amended in 2010 and again in 2019 to address compliance with certain federal regulations, these amendments did not add any of these more substantial issues to the document.

An SLA is crucial to promote continuous and open communication between the parties to the agreement. Without such communication, there is an increased risk the ITSD will not appropriately understand or respond to customer expectations. This weakness could result in confusion or frustration from the customer, or potentially more severe outcomes such as system failure or data loss.

We surveyed officials of consolidated agencies (or divisions of agencies as applicable) to evaluate satisfaction with ITSD services, and to identify concerns over ITSD communication. Responses are summarized in the Appendix. The survey responses indicated while customers worked and communicated well with the front-line ITSD staff, some communications with ITSD could be improved. For example, one respondent mentioned instances in which the ITSD made changes impacting agency systems and data without notifying the agency. In addition, several respondents indicated resource constraints, particularly ITSD staffing, hindered the ability of their agency to use information technology to effectively carry out its mission.

[4] Van Grembergen, Wim, Ph.D., Steven De Haes and Isabelle Amelinckx. "Using COBIT and the Balanced Scorecard as Instruments for Service Level Management." *Information Systems Control Journal*, Volume 4 (2003): 56-62.

According to the *Information Systems Control Journal*,[5] an "SLA is a necessity between a service provider and service beneficiary because a service can be called 'bad' or 'good' only if this service is clearly described. Moreover, it formalizes the needs and expectations of the organization and serves as a kind of guarantee for both parties. In this way, potential misunderstandings are reduced and a clear view is given on the priorities of the service and its delivery. . . . A balanced SLA is a compromise between the needs, expectations and requirements of the organization (user group) and the service provision capabilities and promises of the service provider. At the same time, it must protect the service provider by limiting liability, identifying responsibilities and rationally managing user expectations."

Similar conditions previously reported

During our previous audits of or involving the ITSD, we also noted concerns regarding SLAs. In our 2009 audit of the ITSD consolidation process,[6] ITSD officials indicated the existing SLAs would be reviewed and updated. A 2011 report[7] noted the ITSD had not completed the process of implementing new SLAs with state agency customers. We noted this issue again in our 2012 audit of the ITSD,[8] with ITSD officials again stating they were working on developing "meaningful service level agreements that satisfy both agency and ITSD needs."

Recommendation

The ITSD continue the development of new service level agreements that specify services to be provided and address communications with division customers.

Auditee's Response

ITSD will consider this recommendation but disagrees with the characterization of the lack of such agreements as a finding, as the audit report does not identify any applicable standard or authority requiring the same.

Auditor's Comment

SLAs are common practice between information technology service customers and providers, whether internal or external. Numerous standard-setting organizations provide guidance on SLAs. While not authoritative, we cited the article in the finding because it clearly explains the importance of developing and documenting such agreements.

[5] Ibid.

[6] State Auditor's Office (SAO), Report No. 2009-112, *Office of Administration - Information Technology Consolidation*, issued October 2009.

[7] SAO, Report No. 2011-056, *Department of Revenue - Taxation Division Security Controls*, issued September 2011.

[8] SAO, Report No. 2012-073, *Office of Administration - Information Technology Services Division*, issued July 2012.

2. Contingency Planning Policy

The ITSD has not formally adopted or documented an enterprise-wide contingency planning policy, including overall contingency objectives, an organizational framework, and comprehensive procedures.

Contingency planning is unique to each individual system and agency. As the centralized IT support entity for all consolidated agencies, the ITSD shares responsibility with agency-owners to ensure each system has adequate contingency plans. The ITSD is also consequently responsible for coordinating these plans at an enterprise level to ensure the plans of each system and agency do not conflict, and to align plans to the extent possible to make efficient use of available tools and resources.

While the ITSD has worked with agencies to complete contingency plans for specific agency systems, there is no formal, documented enterprise-wide policy guiding how to develop appropriate, comprehensive contingency plans.

According to accepted standards, information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

Accepted standards further explain that the first step in the contingency planning process is to develop a contingency planning policy statement supported by senior leadership (typically the Chief Information Officer). This policy should define the agency's overall contingency objectives and should establish the organizational framework and responsibilities for information system contingency planning. The policy statement should also address roles and responsibilities. The policy should be supported with procedures covering training requirements, frequency of backups, offsite storage shipments, plan exercises, testing, and maintenance.

Prior SAO audits of specific agency systems have generally found such systems' contingency plans to be adequate. However, without a formally documented enterprise-wide contingency planning policy, there is an increased risk at the enterprise level and in individual system plans that critical components may be overlooked or inadequate, which may negatively impact the state's systems and data; or that existing system and agency plans'

components will be in conflict, causing operational issues in the event multiple plans are exercised.

Recommendation

The ITSD formally adopt and document an enterprise-wide contingency planning policy to ensure appropriate, effective contingency plans are developed for individual agencies and systems, and to guide enterprise-wide decisions.

Auditee's Response

ITSD will consider this recommendation but disagrees with the characterization of the lack of such a policy as a finding, as the audit report does not identify any standard or authority requiring the same.

Auditor's Comment

The standards cited are issued by the National Institute of Standards and Technology (NIST). The specific citations referenced were provided to agency staff during the audit. While compliance with NIST guidance is not required, NIST guidance is considered best practice for many information technology areas, and is frequently cited in internal OA-ITSD security policy documents.

3. Electronic Communication Policy

The ITSD has not developed records management and retention policies in compliance with the Missouri Secretary of State Records Services Division guidance, as approved by the Missouri State Records Commission. This guidance recommends government entities have a policy on electronic messaging, including text messages, email, and other third-party platforms. ITSD officials indicated the division has no policies or procedures regarding communications via text messaging or personal email. As a result, electronic communications may not be retained in accordance with state law.

Section 109.210(5), RSMo, defines a public record as "documents, books, papers, photographs, maps, sound recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or in connection with the transaction of official business." Section 109.270, RSMo, provides that all records made or received by an official in the course of his/her public duties are public property and are not to be disposed of except as provided by law. The guidelines for managing electronic communications records can be found on the Secretary of State's website.[9]

To ensure compliance with state law, the division should develop written policies to address the use of personal email, social media and message accounts, and management and retention of electronic communications.

[9] Missouri Secretary of State Records Services Division, *Electronic Communications Records Guidelines for Missouri Government*, May 14, 2019, is available at <https://www.sos.mo.gov/CMSImages/RecordsManagement/CommunicationsGuidelines.pdf>, accessed October 22, 2020.

Recommendation

The ITSD develop written records management and retention policies to address electronic communications management and retention to comply with Missouri Secretary of State Records Services Division electronic communications guidelines.

Auditee's Response

ITSD will review the cited guidelines but disagrees with the characterization of the lack of such policies as a finding because the audit report does not identify any applicable standard or authority requiring separate policies for record retention based on the format of the record. Existing OA Policy B-36, like Section 109.210(5), RSMo, cited in this recommendation, recognizes that a record may be in a hard copy or electronic form.

Auditor's Comment

When we asked ITSD staff during the audit if any policies related to electronic communications management and retention existed, they indicated "an OA-ITSD policy responsive to your request has not been located." The policy cited by the ITSD in the response provided does not address the management and retention of electronic communications, especially in regards to text messaging, email, and other third-party platforms, but rather addresses public access to records ("Sunshine Law" compliance).

We sent a survey questionnaire to 32 officials of 19 state agencies (or divisions thereof) and indicated they could forward the survey to other staff of their agency who could provide pertinent information. We received 25 responses.

Table 1: Agency user survey results

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
ITSD staff effectively communicate with me.	1	6	3	15	0
ITSD staff respond to my requests for assistance in a timely manner.	2	4	6	10	3
ITSD staff's backgrounds, skill sets, and staffing are adequate to support my needs.	1	4	10	8	2
ITSD provides appropriate security training for my agency's users.	1	1	3	13	7
I know the services available to me from the ITSD.	1	3	7	12	2
I know (and am able to control) the costs of the services ITSD provides.	3	9	4	3	1
ITSD works with me to ensure my needs are met in an efficient and effective manner.	1	5	7	10	2
I have confidence in the actions ITSD takes to adequately secure my systems and data.	3	2	3	15	2
I understand my roles and responsibilities and those of ITSD in regards to managing my systems and data.	1	3	2	17	2
ITSD provides me with the information I need to meet applicable reporting requirements.	0	2	8	11	1
ITSD works proactively to help us improve our data and systems, such as by suggesting upgrades or better solutions to our needs.	1	4	11	6	3

Source: State Auditor's Office (SAO) compilation of returned survey responses. Certain responders did not respond to one or more questions.

The survey also included the following long-form response questions.

Table 2: Additional survey questions

	Number of Responses
Please describe ITSD's communication with your agency. How is ITSD communicating well, and how could their communication be improved?	22
Please describe any areas where you feel ITSD does a particularly good job providing services to your agency.	21
Please describe any concerns you have with the services ITSD provides to your agency.	21
Please provide any other comments you have regarding ITSD or this survey.	15

Source: SAO compilation of returned survey responses. Certain responders did not respond to one or more questions.