Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued January 26, 2017

Massachusetts Housing Finance Agency

For the period July 1, 2014 through December 31, 2015

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

January 26, 2017

Mr. Timothy C. Sullivan, Executive Director
Massachusetts Housing Finance Agency
One Beacon Street
Boston, MA 02108

Dear Mr. Sullivan:

I am pleased to provide this information technology general control audit of the Massachusetts Housing Finance Agency. This version of the report is the limited version that we are issuing publicly; it excludes findings that present information that we believe may be a threat to cyber security. As you are aware, we have also given your agency a copy of the complete report.

This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2014 through December 31, 2015. My audit staff discussed the contents of this report with management of the agency, whose comments are reflected in this report.

I would also like to express my appreciation to the Massachusetts Housing Finance Agency for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CIO	chief information officer
COBIT	Control Objectives for Information and Related Technologies
ISACA	Information Systems Audit and Control Association
ISP	information security program
IT	information technology
ITGC	information technology general control
MassHousing	Massachusetts Housing Finance Agency
MassIT	Massachusetts Office of Information Technology
NIST	National Institute of Standards and Technology
SOC 2 Type 1	Service Organization Control 2 Type 1
SOC 2 Type 2	Service Organization Control 2 Type 2

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted an audit to review and evaluate controls over selected information technology (IT) operations and activities at the Massachusetts Housing Finance Agency (MassHousing) for the period July 1, 2014 through December 31, 2015. Because of the results of our audit planning procedures, it was necessary to extend our audit period to April 14, 2016 in the area of asset inventory.

According to its website, "MassHousing was created by an act of the Massachusetts Legislature in 1966 as an independent public authority charged with increasing affordable rental and for-sale housing in Massachusetts," and it provides "financing for the construction and preservation of affordable rental housing, and for affordable loan products for homebuyers and homeowners."

Our audit of MHFA identified seven findings, but only five are disclosed in this public report. The other two findings have been omitted from this report in accordance with Exemption (n) of the Commonwealth's public records law (Section 7[26][n] of Chapter 4 of the General Laws), which allows for the withholding of certain records, including security measures, or any other records related to cybersecurity or other infrastructure, if their disclosure is likely to jeopardize public safety or cybersecurity.

In accordance with Sections 7.39–7.43 of the Government Accountability Office's *Government Auditing Standards*, as well as the policies of the Office of the State Auditor, for reporting confidential and sensitive information, we have given a separate full report to MFHA, which will be responsible for acting on our recommendations.

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1a **Page 11**	MassHousing did not have a formally documented IT strategic plan.
Finding 1b **Page 12**	MassHousing did not have formally documented IT policies and procedures.
Finding 1c **Page 12**	MassHousing did not perform a data inventory or have a data-classification scheme.
Recommendations **Page 13**	1. MassHousing should formally document an IT strategic plan to manage and direct all IT resources in line with its business strategies and objectives. 2. MassHousing should modify its information security program (ISP) and create policies to include all functions such as physical access security, retention and restoration of data, and data classification. 3. MassHousing should perform a data inventory and develop a data-classification scheme.
Finding 2a **Page 15**	MassHousing could not provide documentation of testing of its disaster-recovery plan, including testing of equipment.
Finding 2b **Page 16**	MassHousing could not provide a current contract with a service provider.
Finding 2c **Page 17**	MassHousing did not receive reports regarding its service provider's information-security measures.
Recommendations **Page 18**	1. MassHousing should conduct and document an annual disaster-recovery test, including testing of mission-critical applications and recovery resources with all employees at the hot site. 2. MassHousing should repair or replace its Incident Management Team's nonfunctioning laptop. 3. MassHousing should review and update the contract for service of backup media and implement a control to periodically review and update all service-provider contracts, including reviews and updates when there is a change in ownership. 4. MassHousing should establish policies and procedures that require the appropriate agency staff members to periodically request and review the Service Organization Control 2 Type 2 report from the contractor that administers its service provider's data center.

Finding 3a **Page 20**	MassHousing did not have an up-to-date Fixed Asset Procedural Manual.
Finding 3b **Page 20**	MassHousing's inventory system contained inaccurate and incomplete entries.
Finding 3c **Page 21**	There are deficiencies in MassHousing's process for removing protected information from IT assets.
Recommendations **Page 23**	1. MassHousing's Administration Division should update its manual to reflect its current inventory system of record. 2. MassHousing should require the Administration Division to conduct an annual inventory of all IT assets. 3. MassHousing management should periodically review the inventory list to ensure that critical data such as location and custodian are captured and accurate and that items are inventoried. 4. MassHousing should retain the disposal log documenting the removal of data from IT assets and the disposal of the assets. 5. MassHousing's IT Department should segregate the duties of removing data from IT assets and notifying the Administration Division that the removal has been performed.
Finding 4a **Page 24**	Employees did not receive IT security training before they were given access to MassHousing's protected information.
Finding 4b **Page 26**	MassHousing did not ensure that all employees, including contractors and interns, signed forms acknowledging that they had read its ISP.
Recommendations **Page 27**	1. MassHousing should train the new employees who have not completed security training. 2. MassHousing should review the training log periodically and implement appropriate controls to ensure that all employees are trained before they are given access to protected information. 3. MassHousing should establish and implement effective policies, procedures, and monitoring controls to ensure that all employees, contractors, and interns sign acknowledgment forms before they are given access to protected information.
Finding 5 **Page 27**	MassHousing did not have adequate controls for its backup schedule.
Recommendations **Page 28**	1. MassHousing should establish access-security policies that state the requirements for managing accounts. These policies should include the requirements to enable it to identify users uniquely. 2. MassHousing should add the user accounts of the staff members who are responsible for the backup schedule to the backup operation group.

OVERVIEW OF AUDITED ENTITY

The Massachusetts Housing Finance Agency (MassHousing) was established by Chapter 708 of the Acts of 1966, as amended, as an independent, quasi-public agency. It is governed by a nine-member board of directors. According to its website, MassHousing's mission is as follows:

> *MassHousing will confront the housing challenges facing the Commonwealth to improve the lives of its people*.

MassHousing does not receive state funding for its operations. According to its website,

> *The Agency raises capital by selling bonds and lends the proceeds to low- and moderate-income homebuyers and homeowners, and to developers who build or preserve affordable and/or mixed-income rental housing. . . . Since its inception, it has provided more than $18.5 billion for affordable housing.*

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted an information technology general control (ITGC) audit of the Massachusetts Housing Finance Agency (MassHousing) for the period July 1, 2014 through December 31, 2015. Because of the results of our audit planning procedures, it was necessary to extend our audit period to April 14, 2016 in the area of asset inventory.

ITGCs are a subset of internal controls that are applied to every information technology (IT) system that an organization relies on and to the IT staff that administers those systems. They provide management and stakeholders with assurance regarding the reliability of data and information systems. The objective of ITGCs is to ensure the confidentiality, integrity, and availability of systems, programs, data files, and computer operations in an organization.

We conducted this ITGC audit in accordance with generally accepted government auditing standards. 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.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	**Conclusion**
Has MassHousing established adequate internal controls to support its mission-critical and essential application systems (i.e., systems essential to its operations) over the following areas?	
a. IT organization and management in regard to IT policies and procedures, IT risk assessments, and providing adequate IT oversight	**No; see Finding 1**
b. IT computer operations such as backup scheduling and network monitoring	**No; see Finding 2**

Objective	Conclusion
c. business continuity and disaster recovery, including its policies and procedures, emergency contact list, hot site,[1] and incident testing	**No; see Finding 2**
d. asset inventory, including inventory management, loss prevention, and disposal management	**No; see Finding 3**
e. protected information,[2] such as employee acknowledgement forms, employee training, and established confidentiality agreements between contractors, vendors, and other third parties	**No; see Finding 4**
f. IT system development and change management, including project approval by IT management and segregation of duties between the testing environment and the production environment	**Yes**
g. logical access security, including background checks, user account management, and password security	**No; see Finding 5**

We conducted this performance audit using criteria from MassHousing's information security program (ISP), which documents how MassHousing keeps data secure and reduces the risk of unauthorized data disclosure. If MassHousing's ISP was deficient in a certain area, we relied on industry standards established by the Information Systems Audit and Control Association (ISACA) in Control Objectives for Information and Related Technologies (COBIT) 4.1, by the National Institute of Standards and Technology, and by the Massachusetts Office of Information Technology. Although MassHousing is not required to follow these industry standards, we believe they represent IT industry best practices for ITGCs. For example, the purpose of COBIT is to provide management and business process owners with an IT governance model that helps in delivering value from IT and understanding and managing the risks associated with IT. According to ISACA's website,

> *COBIT helps bridge the gaps among business requirements, control needs and technical issues. It is a control model to meet the needs of IT governance and ensure the integrity of information and information systems.*

In addition, as part of our review of internal control procedures performed within the context of our audit objectives, we noted that MassHousing did not have an internal control plan. We gained an understanding

[1] A hot site is an offsite location containing all of the equipment an agency would need in order to resume business activities if its primary site became inoperable.

[2] For the purposes of this report, "protected information" is any personal, sensitive, and/or confidential data.

of the internal controls that we deemed significant to our audit objectives through interviews and observations, and we evaluated the design and effectiveness of those controls.

To achieve our objectives, we performed the following audit procedures:

- We assessed MassHousing's controls regarding the oversight of the IT organization and management. Specifically, we performed the following procedures:

    - We requested for review various internal MassHousing documents (including its ISP, IT policies and procedures, IT strategic plan, organization chart, network diagrams, Fixed Asset Procedural Manual, IT steering committee minutes, IT risk assessment reports, and Information Security and Compliance Task Force Charter, as well as various documents related to IT activities) to determine whether MassHousing had adequate IT governance.

    - To determine whether MassHousing had adequate IT oversight of its information, we discussed with management whether MassHousing used a data inventory (a determination of where data is held within the agency and what types of data are held) and data-classification scheme ("an enterprise scheme for classifying data by factors such as criticality, sensitivity and ownership," according to ISACA's website) to accurately identify and classify its data.

- We assessed MassHousing's controls regarding the oversight of computer operation activities for its backup schedule and network monitoring. Specifically, we performed the following procedures:

    - We interviewed managers and a database administrator in the IT Department to obtain an understanding of MassHousing's process for performing backups.

    - We reviewed the shared user account that allowed users to modify the backup schedule for the network and mission-critical applications to determine whether access was uniquely identifiable and based on job responsibilities. We also reviewed the configuration settings for backups to determine whether they were performed daily.

    - We requested the contract with the service provider that maintains MassHousing's backup media storage and retrieval to determine whether it was current and up to date.

    - We inspected email alerts of network system failures to determine whether IT personnel received notifications of system failures.

- We assessed MassHousing's controls to determine whether business continuity and disaster recovery were properly managed. Specifically, we performed the following procedures:

    - We reviewed MassHousing's Disaster Recovery and Incident Management Team Plan to determine whether a hot site had been established, the disaster-recovery plan had been tested, an emergency contact list identified people and businesses to contact in case of a disaster, and the plan was reviewed periodically.

  - We spoke to management about whether they reviewed a Service Organization Control 2 Type 2 report, which details the effectiveness of a service provider's security controls.

- We assessed MassHousing's controls to determine whether its IT asset inventory was being properly managed. Specifically, we performed the following procedures:

  - We obtained and reviewed MassHousing's Fixed Asset Procedural Manual to determine whether it was current and up to date. Also, we conducted interviews with Administration Division personnel to determine whether they periodically reviewed MassHousing's asset inventory system of record.

  - We obtained a list of all assets from MassHousing's system of record and identified IT assets that were within the scope of the audit for inventory testing. We performed data analysis on the information about the assets in this list to identify any missing and/or abnormal data fields.

  - We further examined the inventory list by selecting a sample of 72 inventory items, out of a population of 1,303 items on MassHousing's inventory list, and attempting to verify their physical existence and determine whether they were all correctly recorded on the list. Because our sampling was nonstatistical, we did not project the results of our audit tests to the total populations in the areas we reviewed.

  - We examined a list of IT items disposed of during our audit period and judgmentally selected a sample of 32 out of a population of 200 items to verify that sanitization was performed according to MassHousing's ISP and informal practices. We reviewed documentation to determine whether appropriate approvals from custodians and management were in place to dispose of equipment. Because our sampling was nonstatistical, we did not project the results of our audit tests to the total populations in the areas we reviewed.

- We assessed MassHousing's controls to determine whether protected information was properly safeguarded. Specifically, we performed the following procedures:

  - We interviewed managers in MassHousing's IT and Human Resources Departments to obtain an understanding of MassHousing's process for new employees to complete IT security training and sign acknowledgement forms before gaining access to MassHousing's protected information.

  - We reviewed IT security training logs for all new employees to determine whether they completed training before working with protected information.

  - We reviewed acknowledgment forms for all new employees to determine whether they signed the forms before working with protected information.

  - To verify that MassHousing complied with its ISP, we obtained and inspected confidentiality agreements signed by the companies that provided services related to MassHousing's mission-critical applications.

- We assessed MassHousing's controls to determine whether system development and change management were administered adequately. Specifically, we performed the following procedures:
  - We interviewed managers in MassHousing's IT Department to obtain an understanding of the process for testing and implementing upgrades to MassHousing's mission-critical applications.
  - We observed the testing and production environments to determine whether they were separate.
  - We reviewed MassHousing's Software Development Life Cycle Standard for steps and requirements that MassHousing follows at different phases of software development.
  - We reviewed the management signoff of deployment plans for all of the nine completed patches and upgrades of mission-critical applications from our audit period.
- We assessed MassHousing's controls to determine whether logical access security had been implemented properly for user and administrative accounts. Specifically, we performed the following procedures:
  - We interviewed managers of MassHousing's IT and Human Resources Departments to obtain an understanding of MassHousing's process for approving, changing, and terminating user access accounts to its network and mission-critical applications.
  - We reviewed the background documentation for all new employees to ensure that they had been screened properly before gaining access to MassHousing's mission-critical applications.
  - We reviewed all user access approvals to ensure that all new employees' access to the network had been approved properly.
  - We identified five employees that had transferred from one MassHousing department to another during our audit period; we requested documentation to verify that their access levels had been adjusted properly to reflect their new roles.
  - We reviewed all of the quarterly user access reviews performed by MassHousing personnel for mission-critical applications during the audit period to determine whether user access rights were periodically reviewed and approved by management.
  - We compared an employee termination list to current user lists for mission-critical applications to verify that all terminated employees' accounts had been removed.
  - We obtained screenshots of password parameters for all mission-critical applications, all mission-critical databases, and the network to ensure that they followed the minimum requirements stated by MassHousing.
- We assessed the reliability of the MassHousing data in the inventory system, training system, and human-resource system. Specifically, we reviewed existing information and interviewed knowledgeable staff members about the data. In addition, we performed validity and integrity

tests on all data, including (1) testing for missing data, (2) scanning for duplicate records, (3) testing for values outside a designated range, and (4) looking for dates outside specific time periods. To determine whether the inventory list that we used for asset inventory testing and encryption testing was accurate and complete, we performed a test from the inventory list to each asset's current location and a test of each asset's current location to the inventory list. Based on the analysis conducted, we determined that the data were sufficiently reliable for the purposes of this audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Massachusetts Housing Finance Agency did not have an adequate information technology governance framework.

The Massachusetts Housing Finance Agency (MassHousing) did not have a complete information technology (IT) governance framework that ensured that its IT objectives and activities aligned with its business strategy and overall objectives. Specifically, it did not have a formally documented IT strategic plan, IT policies and procedures, a data inventory, or a data-classification scheme. As a result, there is an increased risk that day-to-day IT operations do not support its overall strategies and objectives.

a. MassHousing did not have a formally documented IT strategic plan.

MassHousing did not have a formally documented IT strategic plan that managed and directed all IT resources in supporting the agency's business strategy and objectives. Without this plan, which is intended to maintain and improve IT process effectiveness and efficiency, there is an increased risk of lost productivity and other problems that a strategic plan could address, such as inadequate data protection.

Strategic plans address issues like data protection, which guards against data breaches that can harm an agency's reputation as well as its finances.

Authoritative Guidance

Adequate IT governance, as described in Section PO1 in Control Objectives for Information and Related Technologies (COBIT) 4.1, includes IT strategic planning:

> *IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realized from project and service portfolios.*

Reasons for Noncompliance

MassHousing's chief information officer (CIO) held periodic IT steering committee meetings that addressed MassHousing's IT strategic plan. However, no such plan was ever formally documented or communicated throughout MassHousing because there was no formal requirement to do this.

b. MassHousing did not have formally documented IT policies and procedures.

MassHousing lacked IT policies and procedures that set requirements addressing all functions, such as physical access security, retention and restoration of data, data inventory, and a data-classification scheme. Without formally documented IT policies and procedures, there was no guidance for employees on how to perform day-to-day functions supporting business operations. This could result in miscommunication and misunderstandings regarding MassHousing's business strategies and objectives.

We requested IT policies and procedures for review, and management provided an information security program (ISP). The ISP is a high-level document that provides guidance on how to safeguard protected information and reduce the risks of unauthorized disclosure, but it does not outline specific tasks employees should do to achieve those goals.

Authoritative Guidance

COBIT 4.1 establishes the process of governance oversight over IT, in keeping with COBIT's purpose as an IT governance framework. Section PO4 of that document describes a proper control system as one in which "processes, administrative policies and procedures are in place for all functions." The "COBIT Framework" section directs organizations to "define and communicate how all policies, plans and procedures that drive an IT process are documented, reviewed, maintained, approved, stored, communicated and used for training."

Reasons for Noncompliance

MassHousing relied on its ISP as its IT policy for all functions and therefore did not develop individual policies and procedures.

c. MassHousing did not perform a data inventory or have a data-classification scheme.

MassHousing did not conduct a data inventory or develop a data-classification scheme, so its data is not identified and classified based on sensitivities, risks, and locations. Without an adequate understanding of the locations and purposes of data, there is an increased risk that MassHousing will not apply sufficient controls to protect personal and confidential data. Compromise of personal and confidential data can seriously damage the mission, safety, or integrity of an agency and its staff.

Authoritative Guidance

Section PO2 of COBIT requires the establishment of a "classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data."

The Massachusetts Office of Information Technology (MassIT) Enterprise IT Asset and Risk Management Policy requires agencies to "maintain an inventory of IT assets which consist of physical IT assets (hardware, network devices, etc.) and logical IT assets (**data**, software, licensing, and applications)." (emphasis added)

Reasons for Noncompliance

MassHousing's management believed that the encryption of data was sufficient to safeguard the protected information in its systems, and therefore the agency did not perform a data inventory or develop and implement a data-classification scheme.

Recommendations

1. MassHousing should formally document an IT strategic plan to manage and direct all IT resources in line with its business strategies and objectives.
2. MassHousing should modify its ISP and create policies to include all functions such as physical access security, retention and restoration of data, and data classification.
3. MassHousing should perform a data inventory and develop a data-classification scheme.

Auditee's Response

MassHousing respectfully disagrees with the State Auditor's assessment that we have not "established adequate internal controls to support the agency's mission critical and essential application systems" in seven out of eight audit objectives. Although MassHousing acknowledges that certain items were identified during the audit engagement, these items do not rise to the level where internal controls are inadequate and risk is not being managed effectively. MassHousing maintains robust internal controls and effectively manages risks related to information technology.

As was discussed with the State Auditor's team, a new Chief Information Officer was hired to lead MassHousing's IT Division prior to the commencement of the audit engagement. A comprehensive review and assessment of MassHousing's IT management and practices has been ongoing since the change in leadership, with deliberate planning and effectiveness. In MassHousing's continuing effort to strengthen its IT Governance Framework, Executive Management has approved a five-year IT Strategic Plan, is instituting an IT Governance Board and Technical Architecture Review Board, and has reorganized IT staff and rolled out a Service Delivery Department and Project

Management Office to help manage and prioritize IT projects and resources. Executive and IT Management are committed to addressing, in the manner deemed most appropriate, all of the issues identified in the State Auditor's findings.

MassHousing notes that the audit team's statement that "MassHousing relied on its ISP as its IT Policy for all functions . . ." is not accurate. MassHousing provided over 330 documents to the audit team during the course of the engagement. It is simply not correct that MassHousing's IT operations are governed only by one policy.

MassHousing was unaware that data inventory or data classification scheme issues were a concern of the State Auditor's team.

Auditor's Reply

Although MassHousing asserts that it maintains robust internal controls and effectively manages risks related to IT, our audit identified significant problems with the agency's IT controls. Specifically, as noted above, MassHousing did not have a complete IT governance framework that ensured that its IT objectives and activities aligned with its business strategy and overall objectives, a fact not disputed by MassHousing. Such a framework would include a formally documented IT strategic plan, IT policies and procedures, a data inventory, and/or a data-classification scheme. Thus, in our opinion, MassHousing had not established adequate internal controls to support its mission-critical and essential application systems. The items discussed in the seven out of eight audit objectives referred to above identify internal control weaknesses according to MassHousing's ISP and industry best practices. Documented IT policies for areas like physical access security, retention and restoration of data, and data inventory; a data-classification scheme; the testing of a disaster-recovery plan; management of fixed assets; proper security training; and physical access controls provide the basis of a system of controls and guidance for day-to-day functions. Without them, MassHousing increases the risk that IT governance is not in place and effective.

MassHousing replaced its CIO to lead MassHousing's IT Division internally, but not before the start of the audit period. We held a meeting with the new CIO about our concerns regarding IT governance. MassHousing gave us a draft of an IT strategic plan, but our testing confirmed that the draft plan had not been implemented. We agree that MassHousing was cooperative in providing requested documents, but our review of these documents and our discussions with agency personnel confirmed that policies for physical access security, retention and restoration of data, data inventory, and a data-classification scheme had not been developed and codified as agency policy. Further, in a meeting with the audit team, the former CIO (who was responsible for the policies in place during the audit period) told us that the ISP covered all areas of the IT policies and that new management would address this issue.

Regarding data inventory and data classification, during our audit, IT management at MassHousing told us that data classification had not been performed on personal identifiable information because MassHousing encrypts all of its data as if it did contain such information. However, as noted in our report, not all devices were encrypted to protect MassHousing's data. Finally, after the end of our audit fieldwork, we emailed MassHousing management to inform them that IT governance covers many areas, including data classification, and that we observed during our audit that MassHousing did not have a data-classification scheme. A data inventory and data-classification scheme would reduce the risk of MassHousing's information being compromised by identifying all types of information collected.

Based on its response, MassHousing is taking steps to address our concerns.

2. MassHousing did not have sufficient management oversight over its service providers.

MassHousing did not sufficiently oversee its service providers. MassHousing contracted with one service provider to supply a hot site (an offsite location containing all the equipment necessary for MassHousing to resume business activities if its primary site became inoperable) for all MassHousing data in case of a disaster. It also contracted with another provider that stores backup media (items, such as compact discs, that hold copies of data for use in the event of a failure or loss) in an offsite location. MassHousing did not perform a disaster-recovery test (a test of each procedure in a disaster-recovery plan) at the hot site, update the contract with the backup-storage provider, or review a report to determine whether the service provider for the hot site maintained effective controls to protect MassHousing's information. As a result, there is an increased risk that restoration of technology operations will be delayed in the event of a disaster. That delay could lead to financial loss and reputational damage.

a. MassHousing could not provide documentation of testing of its disaster-recovery plan.

MassHousing could not provide documentation to verify that disaster-recovery tests had been performed as required by its Disaster Recovery and Incident Management Team Plan (recovery plan). In addition, we determined through an interview that one laptop assigned to a key employee was not functioning. As a result of these issues, MassHousing has inadequate assurance that it could recover all of its mission-critical activities and protected data and continue to operate in the event of a disaster.

MassHousing uses a service-provider data center as a hot site for disaster recovery and emergencies. IT management created a recovery plan for the overall coordination of response and recovery support activities, but has not tested the plan at the hot site to ensure that the plan adequately addresses MassHousing's recovery needs. For instance, MassHousing could not provide documentation that it had performed data retrieval and restoration testing, which evaluates applications' ability to retrieve and restore data in a timely manner, at its hot site.

The nonfunctioning laptop was assigned to a member of the Incident Management Team. According to MassHousing's recovery plan, this team "provides overall coordination of response and recovery support activities" from "any unplanned business interruption, such as loss of utility service, building evacuation, or a catastrophic event such as a major fire or disaster." This laptop supported that function and was stored off site to be used for disaster recovery and emergencies.

Authoritative Guidance

MassHousing's Disaster Recovery and Incident Management Team Plan requires a disaster-recovery test to be conducted and documented annually on all mission-critical applications. It also requires that all offsite equipment to be used for recovery, including records and documentation backups, be tested and documented annually.

Reasons for Issues

The Incident Management Team is responsible for documenting the disaster recovery tests and ensuring the effectiveness of the recovery plan within MassHousing. MassHousing did not prioritize the disaster recovery tests because of a lack of IT governance. The Incident Management Team was unaware of the nonfunctioning laptop (until we requested it in an interview for testing) because MassHousing had not attempted testing of the disaster-recovery plan, which would include testing all equipment stored off site.

b. MassHousing could not provide a current contract with a service provider.

MassHousing could not provide us with a current contract with its service provider for backup media storage. Backup media storage ensures that MassHousing can retrieve and restore its backup media from an offsite location in the event of a disaster. The contract has not been reviewed and updated since 2002, even though the original service company has been acquired by other companies several times since then.

A contract for backup media storage defines the terms, conditions, and service level to be provided. Without a current contract, the contract terms may not reflect the technology and service levels needed to meet all MassHousing's current recovery requirements.

Authoritative Guidance

Section DS1 of COBIT 4.1 requires agencies to do the following:

> *Regularly review [service level agreements] and underpinning contracts . . . with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account.*

Reasons for Out-of-Date Contract

MassHousing's management did not establish policies and procedures that required its staff to periodically review and/or amend the contract or change providers for backup media services when there was a change in ownership.

c. MassHousing did not receive reports regarding its service provider's information-security measures.

MassHousing did not receive reports that detailed the effectiveness of its service provider's information-security controls. Specifically, it did not obtain and review a Service Organization Control 2 Type 2 (SOC 2 Type 2) report, which would detail the effectiveness of security controls, from the service provider even though one had been completed by an independent public accounting firm and was available for MassHousing's review. MassHousing did obtain a Service Organization Control 2 Type 1 (SOC 2 Type 1) report, which is a high-level document detailing whether controls are properly designed, but that type of report does not include assessments of whether the controls are effective.

Without obtaining and reviewing a SOC 2 Type 2 report, MassHousing could be unaware of any weaknesses at its service provider's data center that could lead to unauthorized disclosure or alteration of protected information.

Authoritative Guidance

Section IV(C) of MassHousing's ISP requires an assessment of the effectiveness of a service provider's IT controls:

> *In the event that the reports or tests indicate that such vendor's information security measures are inadequate or otherwise put MassHousing's Protected Information at risk, MassHousing's Director of Information Technology shall report such results to MassHousing's General Counsel and Chief Administrative Officer, and they shall either take appropriate steps to cause the vendor to remedy the deficiency or terminate the arrangement.*

Without reports that indicate the effectiveness of IT controls from the service provider's data center, MassHousing cannot fulfill this requirement.

Reasons for Lack of Oversight

MassHousing's management did not establish policies and procedures that assigned responsibilities to staff members to periodically review the effectiveness of the information security measures of its service provider's data center.

Recommendations

1. MassHousing should conduct and document an annual disaster-recovery test, including testing of mission-critical applications and recovery resources with all employees at the hot site.
2. MassHousing should repair or replace the Incident Management Team laptop.
3. MassHousing should review and update the contract for service of backup media and implement a control to periodically review and update all service-provider contracts, including reviews and updates when there is a change in ownership.
4. MassHousing should establish policies and procedures that require the appropriate agency staff members to periodically request and review the SOC 2 Type 2 report from the contractor that administers its service provider's data center.

Auditee's Response

MassHousing has successfully tested its abilities to retrieve electronic data for continued operations at its disaster (hot) site, with the last test during the audit period occurring in March 2015. The next level of disaster recovery (DR) planning, in which all required personnel participates, utilizing all the necessary equipment, to ensure business continuity in the event of a disaster impacting MassHousing's operations, should be completed and the results reported to the Investment and Audit Committee of MassHousing's Board by the close of FY17 (June 30, 2017).

The laptop, noted as part of the Incident Management Team, has been retired and the requirement that a team member carry a laptop in their vehicle has been eliminated.

MassHousing understands the importance of having current contracts in place with its vendors. With respect to the backup media storage company, MassHousing's contract with this vendor was in effect at all times, as the contract applied to the original vendor's legal successors. Although not legally required, MassHousing has executed a replacement contract with the vendor at the suggestion of the audit team. In addition, a documented process will be implemented whereby all IT goods and services contracts are reviewed on a periodic basis. This process is planned to be operational by October 31, 2016.

MassHousing has consistently received and reviewed all SOC2 Type 1 reports available from its service providers. The State Auditor's requirement that we begin receiving SOC2 Type 2 reports may not be possible or appropriate in all situations. The SOC2 Type 2 report is not an industry standard, mainly due to the cost of this type of report, and may not be available from all of our service providers. MassHousing will continue to work with its service providers to obtain the most relevant and beneficial information available.

Auditor's Reply

Despite its assertion, MassHousing did not give us documentation during the audit to show that disaster-recovery tests had been performed as required by its recovery plan. Annual disaster-recovery tests, which are key to ensuring that MassHousing would be able to recover all of its mission-critical activities and protected data and continue to operate in the event of a disaster, should be documented and all necessary equipment tested.

We cannot comment on MassHousing's assertion that its contract with the backup media storage vendor was in effect at all times. However all MassHousing's vendors should have valid, up-to date contracts that identify current scopes of services so that the contracts can be properly administered.

We agree that MassHousing received a SOC 2 Type 1 report, as mentioned in our finding. However, there was no verifiable evidence that these reports had been reviewed by MassHousing and changes implemented when necessary. Since the service provider we mentioned in connection to this matter is responsible for business continuity in the event of a disaster, it is essential that MassHousing verify that the service provider has effective controls. A SOC 2 Type 2 report would provide assurance that MassHousing's data centers were managed effectively.

Based on its response, MassHousing is taking steps to address our concerns.

3. MassHousing did not properly manage its IT assets.

MassHousing did not properly administer its inventory of IT assets. Specifically, it did not have an up-to-date Fixed Asset Procedural Manual or an accurate and complete inventory system of record, and there were deficiencies in its process for ensuring that protected information is removed from IT assets before they were disposed of. This increases the risk of theft and misuse of IT assets and unauthorized use of any protected information stored on them.

a. MassHousing did not have an up-to-date Fixed Asset Procedural Manual.

MassHousing's Fixed Asset Procedural Manual was not up to date with regard to its current inventory system. This manual describes the IT inventory process, including how assets are recorded, controlled, and disposed of. It was last updated in 2005 and describes procedures for an inventory system that is no longer being used. MassHousing implemented a new inventory system in 2014 and did not update its manual. For example, the manual does not define the dollar value of the IT assets that have to be inventoried, the frequency of the inventory, or how the inventory is to be documented. Therefore, there is no documentation of MassHousing's current inventory system and process that management can use to implement proper control over agency's IT assets to prevent theft and misuse.

Authoritative Guidance

COBIT 4.1 requires that an organization's "policies, plans and procedures [be] accessible, correct, understood and up to date."

Reasons for Noncompliance

MassHousing officials stated that they do not periodically review the manual to ensure that it is up to date. The agency did not establish requirements to ensure that its manual was periodically reviewed and properly updated as necessary. The officials could not explain why the manual had not been updated when the agency converted to the new inventory system.

b. MassHousing's inventory system contained inaccurate and incomplete entries.

MassHousing did not conduct an annual inventory of IT assets and therefore had inaccurate and incomplete information in its inventory system. Not having complete and accurate inventory records places MassHousing's IT assets at greater risk of theft or misuse.

Specifically, for 309 (24%) of MassHousing's total population of 1,303 IT assets, the listed location was a room that was no longer part of MassHousing. For example, 20 of these assets were identified as located in New Jersey at a MassHousing disaster-recovery site that, according to agency records, has not been used by MassHousing in more than four years. In addition, 181 (14%) of the 1,303 IT assets did not have an assigned custodian or data owner (i.e., a person who was responsible for their protection).

Authoritative Guidance

MassIT's Enterprise IT Asset and Risk Management Policy requires agency staff to do the following:

> *1.1.2 Identify the location—physical or logical—of the asset. . . .*
>
> *1.1.5 Identify the data owner for each asset with responsibility for ensuring that: the asset is correctly classified . . .*
>
> *1.1.7 Annually conduct a physical audit of IT assets and reconcile the audit with the IT asset inventory. Agencies must investigate and resolve discrepancies between the physical audit of IT assets and the IT asset inventory.*

Reasons for Noncompliance

MassHousing did not establish policies and procedures to ensure that the information about IT assets in its inventory system was complete and accurate. According to MassHousing officials, the information in the system was only updated when the IT Department asked the Administration Division to update the location or change the custodian of an asset. The Administration Division pointed out to us that a periodic inventory of IT assets (which could have revealed the inaccuracies) was not required by MassHousing policy and no inventory had ever been performed.

c. There are deficiencies in MassHousing's process for removing protected information from IT assets.

MassHousing did not adequately document that all protected information was removed from IT assets before they were disposed of and did not adequately segregate the duties of employees who were responsible for removing protected information from its IT assets. As a result, there is a higher-than-acceptable risk that protected information on MassHousing's IT assets will be subject to unauthorized access, waste, fraud, or misuse.

We obtained from MassHousing a list of all 200 IT assets that MassHousing designated as disposed of during our audit period. We judgmentally selected 32 of these IT assets to test in order to determine whether adequate documentation existed that all protected information had been removed from them before they were disposed of. According to agency officials, when IT assets were to be disposed of, the IT Department was to sanitize (i.e., remove) all protected information from them and then submit disposal logs to notify the Administration Division that the assets were ready for disposal. MassHousing could not provide disposal logs for 9 (28%) of 32 assets to show that the IT Department had informed the Administration Division that all data had been removed from them. Without the disposal logs, the Administration Division could not provide evidence that all protected information had been removed from the assets.

In addition, the IT Department's duties for this activity were inadequately segregated: the same person was responsible for removing the protected information and notifying the Administration Division. Thus there is no process whereby someone independently checks the IT assets being disposed of to ensure that all protected information has been removed.

Authoritative Guidance

Section III(B) of MassHousing's ISP states,

> *When disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that may contain Protected Information, all data must be erased.*

In its document *Guidelines for Media Sanitization*, the National Institute of Standards and Technology (NIST) states,

> *It is critical that an organization maintain a record of its sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media. Often when an organization is suspected of losing control of its information, it is because of inadequate record keeping of media sanitization.*

Section 3 of MassIT's Enterprise Communications and Operations Management Policy states,

> *Separation or segregation of duties is a method for reducing risk of accidental or deliberate system misuse by segregating an individual staff member's (including but not limited to employee, contractor, etc.) sphere of influence and control, and must be applied to the extent possible and practicable to all IT systems particularly those that collect, handle, store, process, dispose, or disseminate high sensitivity data.*

Reasons for Noncompliance

MassHousing's manual did not develop detailed guidelines for the sanitization and disposal process to establish the roles and responsibilities of each department or the requirement of documentation.

Recommendations

1. MassHousing's Administration Division should update its manual to reflect its current inventory system of record.
2. MassHousing should require the Administration Division to conduct an annual inventory of all IT assets.
3. MassHousing management should periodically review the inventory list to ensure that critical data such as location and custodian are captured and accurate and that items are inventoried.
4. MassHousing should retain the disposal log documenting the removal of data from IT assets and the disposal of the assets.
5. MassHousing's IT Department should segregate the duties of removing data from IT assets and notifying the Administration Division that the removal has been performed.

Auditee's Response

The procedures outlined in MassHousing's Fixed Asset Procedures Manual remain applicable despite MassHousing's change in fixed asset management software. The Manual's instructions do not depend on using a specific software package, but rather outline the required process through specified terms, definitions and workflow diagrams. MassHousing intends to complete a review of its Fixed Asset Procedures Manual by October 31, 2016, and will make any appropriate updates as part of that review. MassHousing will develop an ongoing quality control function, supported by inventory management reporting, to reduce potential location or custodian errors. This will be augmented by an annual fixed asset inventory that is scheduled to be completed by the close of FY17 (June 30, 2017).

With respect to disposal of computer equipment containing potential protected information, although the audit team was not satisfied with MassHousing's paper and electronic support around this process, this does not mean that the staff performing the disposals were not effectively executing their responsibilities, using required processes and equipment. MassHousing IT, along with the Administration Division, is currently reviewing its processes for removing protected information and disposing of computer equipment to ensure that the proper procedures and controls are applied and documented consistently. This review process should be completed by October 31, 2016.

Auditor's Reply

As noted above, MassHousing's Fixed Asset Procedural Manual was not up to date with regard to the agency's current inventory system: it was last updated in 2005 and described procedures for an inventory system that is no longer used. MassHousing implemented a new inventory system in 2014 and did not update its manual; therefore, there is no documentation of its current inventory system or of a process that management can use to implement proper control over the agency's IT assets to prevent theft and misuse. MassHousing intends to complete and review its Fixed Asset Procedure Manual as a move toward more efficient management of IT assets. Updating the manual when a new system is implemented is essential to ensure that the fixed-asset inventory is accurate and that it accounts for such things as a properly defined dollar value of IT assets, the frequency of the inventory, and how the inventory is to be documented. A system of quality control is essential in ensuring that the annual inventory is accurate.

According to its response, MassHousing is reviewing its processes for removing protected information and disposing of computer equipment to ensure that the proper procedures and controls are applied and documented consistently. Documenting that assets were disposed of reduces the risk that protected information on MassHousing's IT assets will be subjected to unauthorized access, waste, fraud, or misuse and ensures the accuracy, tracking, and monitoring of inventory.

Based on its response, MassHousing is taking steps to address our concerns.

4. MassHousing did not have sufficient controls over the security and confidentiality of protected information.

MassHousing did not have sufficient controls over the security and confidentiality of protected information. Specifically, it did not ensure that all employees completed IT security training before they were given access to MassHousing's protected information or that they signed an acknowledgement form verifying that they had received the ISP. Thus MassHousing is not properly safeguarding its protected information against possible misuse.

a. Employees did not receive IT security training before they were given access to MassHousing's protected information.

In reviewing the training logs for the 67 employees hired during the audit period (who included full-time employees, interns, and contractors), we found that none of them completed IT security training before gaining access to MassHousing's protected information.

Over the course of our audit period, MassHousing security training operated under two unwritten practices. Management explained that under the old practice, from July 1, 2014 through October 30, 2015, security training was to be provided each year in February to full-time employees only. They also explained to us that under the new practice (after October 30, 2015 for full-time employees and November 24, 2015 for interns and contractors), security training was to occur shortly after hire. However, they did not define "shortly." Both practices were inadequate, since they allowed personnel to access MassHousing's protected information without receiving security training, sometimes for extended periods, as noted below.

- As of the date of our testing, 64 out of the 67 employees hired during the audit period were hired under the old practice. Of these 64 employees, 22 (34%) had never completed the required security training. This resulted in personnel having access to MassHousing's protected information for 1 to 11 months without receiving security training. Seven of the 22 employees were active employees as of the date of our testing (March 2016), and even after the training policy was updated, they still did not complete security training.
- As of the date of our testing, 3 out of 67 employees hired during the audit period were hired under the new practice. Of these 3 employees, 2 (67%) gained access to protected MassHousing information for 22 to 30 days before completing security training. In addition, 1 (33%) of the 3 employees never completed the training because he left MassHousing before receiving training. A training notice was sent to this employee 9 days after he was hired, but he never completed training and thus had access to MassHousing's protected information for approximately two months without receiving security training.

Authoritative Guidance

Massachusetts Executive Order 504 states,

> *All agency heads, managers, supervisors, and employees (including contract employees) shall attend mandatory information security training within one year of the effective date of this Order. For future employees, such training shall be part of the standardized orientation provided* ***at the time they commence work.*** [emphasis added]

Reasons for Late Training

MassHousing could not provide a reason that training was only offered once a year under the old practice or that no specific timeframe for training was prescribed under the new practice. When MassHousing changed its training practice in October 2015, which requires all new hires to receive security training shortly after hire, MassHousing did not establish and implement effective policies, procedures, and monitoring controls such as reviewing the training log to ensure that employees were trained prior to gaining access to protected information.

b. MassHousing did not ensure that all employees, including contractors and interns, signed forms acknowledging that they had read its ISP.

MassHousing did not ensure that all employees, contractors, and interns signed acknowledgment forms to confirm that they had received and read its ISP before it gave them access to its protected information. Our review of the acknowledgement forms for the 67 employees, contractors, and interns hired during our audit period showed that 43 (64%) of them did not sign the forms. Further, some people signed them late. For example, 5 (7%) of the employees' acknowledgement forms were signed as many as 31 days after their hire dates.

A signed acknowledgement form provides assurance to MassHousing that an employee has read, understands, and agrees to abide by the rules set forth in the ISP. Without signed forms, MassHousing would not know whether all its employees knew the rules set forth in its ISP and understood how to protect its information.

Authoritative Guidance

Section III(A) of MassHousing's ISP requires the following for its employees and contractors:

> *All employees will from time to time be required to acknowledge that they have read and will comply with MassHousing's confidentiality and security standards for handling Protected Information.*

Appendix F of Revision 4 of NIST's Special Publication 800-53 describes a properly functioning organization as follows:

> *The organization . . . ensures that individuals requiring access to organizational information and information systems . . . sign appropriate access agreements prior to being granted access . . . . Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized.*

Reasons for Deficiencies

MassHousing had not established and implemented effective policies, procedures, and monitoring controls that required and ensured that all employees, contractors, and interns signed acknowledgement forms before they were given access to protected information.

Recommendations

1. MassHousing should train the new employees who have not completed security training.
2. MassHousing should review the training log periodically and implement appropriate controls to ensure that all employees are trained before they are given access to protected information.
3. MassHousing should establish and implement effective policies, procedures, and monitoring controls to ensure that all employees, contractors, and interns sign acknowledgment forms before they are given access to protected information.

Auditee's Response

> *MassHousing was an early adopter of applicable information security protocols as evidenced in its publishing of its Information Security Program. Other information security measures implemented include, but are not limited to, security awareness training, identification of "privacy officers," formation of an "information security taskforce," encryption of portable devices, and the encryption of protected information sent in all Agency emails. MassHousing recognizes that training new employees upon arrival as opposed to the next scheduled Agency-wide training offering would increase our new employees' awareness and obligation to safeguard protected information. Management is planning to implement a process to ensure initial, day-one security awareness training for all new hires with access to our IT network by October 31, 2016.*
>
> *With the adoption of initial, day-one training, MassHousing is committing to obtaining timely acknowledgments from new employees, including interns, temporary personnel and contractors, that they have read the Agency's Information Security Program. This practice is expected to be operational by October 31, 2016.*

Auditor's Reply

MassHousing's implementation and documentation of IT security training for all employees, temporary personnel, and contractors who have access to its systems is key to ensuring that its systems are properly safeguarded.

5. MassHousing did not have adequate controls for its backup schedule.

MassHousing did not have adequate controls over who could access the system account that controlled the backup schedule for its systems. A backup schedule is a routine that sets the time and location for copies of data to be created and available for use in the event of a failure or loss. Specifically, MassHousing has one system account that, according to IT Department management, was shared among four IT Department employees. The system could not detect which of these four employees accessed the account and the backup schedule at any given time.

Without adequate controls, the system lacked a mechanism for establishing accountability, which increases the risk of an employee being able to change the backup configuration settings (such as the backup schedule) without being detected. This could result in a loss of files and data.

Authoritative Guidance

As previously mentioned, Section DS5 of COBIT 4.1 requires organizations to ensure that users and their activities are uniquely identifiable.

Reasons for Inadequate Controls

MassHousing did not use the capability to add multiple uniquely identifiable users to the backup operation group (the group of users who can modify the backup schedule). It also did not establish access-security policies that prohibited the sharing of accounts. MassHousing's IT management gave access to the backup schedule to multiple IT staff members via a single account because it was more convenient.

Recommendations

1. MassHousing should establish access-security policies that state the requirements for managing accounts. These policies should include the requirements to enable it to identify users uniquely.
2. MassHousing should add the user accounts of the staff members who are responsible for the backup schedule to the backup operation group.

Auditee's Response

MassHousing IT has made the appropriate changes to the backup operations group, and each system-level account is held by an individual IT Division employee. MassHousing follows a "uniquely identifiable" user account practice for all of its key financial applications and places strict controls on access to unassigned system service accounts. As part of the policy and procedure review noted in Finding no. 1, MassHousing will consider if any changes are appropriate in the context of this finding.

Please note that with respect to all key financial applications, an unassigned system service account requires an application owner (i.e. Division Director) to grant access to that account. These accounts are subject to quarterly review by Management, including IT, and MassHousing's Internal Audit Department.

Auditor's Reply

We believe MassHousing is taking the appropriate steps to control its backup schedule adequately. Establishing accountability and a level of review will reduce the risk of employees' being able to change the backup configuration settings without being identified.