PERFORMANCE AUDIT

Office of the Washington State Auditor
Pat McCarthy

Data Backup and Disaster Recovery

September 17, 2020

Report Number: 1026917

Table of Contents

State Auditor's Office contacts

State Auditor Pat McCarthy
564-999-0801, Pat.McCarthy@sao.wa.gov

Scott Frank – Director of Performance and IT Audit
564-999-0809, Scott.Frank@sao.wa.gov

Christopher Cortines, CPA – Assistant Director for Performance Audit
206-355-1546, Christopher.Cortines@sao.wa.gov

Shauna Good – Principal Performance Auditor
564-999-0825, Shauna.Good@sao.wa.gov

Diana Evans, CPA – Lead IT Auditor
564-999-0952, Diana.Evans@sao.wa.gov

Kathleen Cooper – Director of Communications
564-999-0800, Kathleen.Cooper@sao.wa.gov

To request public records

Public Records Officer
564-999-0918, PublicRecords@sao.wa.gov

Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email *Webmaster@sao.wa.gov* for more information.

Executive Summary

Background (page 6)

Washington state agencies are required to keep their data and information technology (IT) systems safe from a variety of events including network outages, security incidents, and natural disasters. Being unprepared for these events can lead to a disruption of critical state services, lost revenue and records, and reduced organizational effectiveness.

This audit looked at two areas: data and system backup and disaster recovery. A backup is simply a copy of your data or system. A disaster recovery plan sets out, in policies and procedures, how you will recover data and restore full system operations to ensure business continuity. Earlier audits performed by the Office of the Washington State Auditor found agencies usually had data backup procedures, but did not consistently perform tests to verify they could restore critical data. Furthermore, even fewer had a current and tested disaster recovery plan.

This audit evaluated whether four state agencies had proper backup strategies and disaster recovery procedures in place, including testing the plan, for selected systems. We compared our observations to state requirements and leading practices. The audit identified key areas for improvement to help agencies better prepare for potential future incidents.

Audited agencies can improve their ability to restore critical systems and data in the event of a disaster or security incident (page 10)

None of the four audited agencies fully and consistently met all state requirements for data backup, disaster recovery and testing recovery plans. In addition to meeting state requirements, agencies could further reduce disruptions to their services and operations by following the backup and disaster recovery guidance offered by leading practices.

Audited agencies lacked the resources and guidance they needed to establish comprehensive backup and disaster recovery practices and procedures (page 17)

Executive managers at some agencies were not always aware of all risks and potential consequences, and so did not always allocate adequate resources to address the risks. We found none of the four audited agencies adequately used IT risk assessments and business impact analyses to identify and inform management of the risks. Executive management's investment in technology and staff is nonetheless key to implementing effective backup strategies and disaster recovery plans. Better statewide guidance and tools could help agencies implement more effective backup strategies and disaster recovery plans.

State Auditor's Conclusion (page 20)

State agencies' ability to provide essential services relies heavily on the availability of a variety of IT systems. Any number of things can happen to interrupt the availability of those systems, including relatively mundane equipment failures, unforeseen natural disasters, or malicious security attacks. When these events happen, it is important for agencies to have reliable backups of their systems and their data, as well as a solid plan to recover their most important systems quickly.

The state's security requirements and other sources of leading practices can help agencies develop effective backup and disaster recovery plans that are tailored to the business needs and risks each agency faces. In the appendices of this report, we have compiled those requirements and leading practices in one place. These are important resources, and we would encourage all state agencies to take advantage of them as they develop their own recovery plans.

Recommendations (page 21)

We gave detailed recommendations to the four agencies that addressed three issues:

- Using IT risk assessments and business impact analyses to identify gaps in current backup and disaster recovery practices and procedures
- Ensuring management is aware of issues affecting data backup and disaster recovery efforts, so they can adequately address them

- Implementing backup and disaster recovery procedures and processes that align with state requirements and leading practices

We further recommended the Office of the Chief Information Officer help agencies develop more effective and comprehensive backup and disaster recovery processes by providing clear and up-to-date guidance.

We also suggested all Washington state agencies consider the general recommendations included in this report and use leading practices as they implement backup and disaster recovery programs. This audit may also offer useful guidance to local governments.

Next steps

Our performance audits of state programs and services are reviewed by the Joint Legislative Audit and Review Committee (JLARC) and/or by other legislative committees whose members wish to consider findings and recommendations on specific topics. Representatives of the Office of the State Auditor will review this audit with JLARC's Initiative 900 Subcommittee in Olympia. The public will have the opportunity to comment at this hearing. Please check the JLARC website for the exact date, time, and location (www.leg.wa.gov/JLARC). The Office conducts periodic follow-up evaluations to assess the status of recommendations and may conduct follow-up audits at its discretion. See **Appendix A**, which addresses the I-900 areas covered in the audit. **Appendix B** contains information about our methodology.

Background

Washington state agencies depend on information technology (IT) systems to perform a variety of critical functions, including public safety, social services, tax collection and transportation. These IT systems, and the data they process, must be kept stable, secure and complete if they are to help ensure the safety and well-being of Washingtonians. Security incidents and natural disasters can render key data and systems unavailable, risking the ability of government agencies to deliver services.

IT security incident

Any unplanned or suspected event that could jeopardize the confidentiality, integrity or availability of IT systems and data.

Natural disaster

Includes earthquakes, forest fires, floods, and other severe conditions that can damage data centers, resulting in the loss of data and system services.

At any time, data may be lost, stolen or modified due to accident, disaster, negligence or intentional attack. Washington is already susceptible to a variety of natural disasters, possessing active and dormant volcanoes, straddling earthquake fault lines, and prone to both flooding and wildfires. Regional disasters such as these can take down critical systems supporting public safety and wellness, as well as result in loss of revenue due to systems unable to receive payments or process financial transactions. In a worst-case scenario, agencies may not be able to recover critical systems and have to rebuild from scratch.

Furthermore, government organizations are attractive targets for malicious attacks such as ransomware. Governments that have been successfully attacked are often faced with an unpalatable choice: Fail to deliver services or pay an expensive ransom to the hacker in the hope of retrieving the data. Since 2017, the United Kingdom's National Health Service, Garfield County in Utah, and 22 municipalities in Texas, to name just a few, were attacked with ransomware that severely disrupted operations. Ransomware attacks occurring in March 2018 cost the city of Atlanta at least $17 million, while in May 2019, another ransomware attack hit the city of Baltimore at a cost of more than $18 million. These types of incidents can lead not only to the loss of funds, but the loss of financial, legal and public records, and decreased organizational effectiveness.

Governments large and small must ensure they can keep functioning properly no matter what happens. Key to the continued operation of critical government functions is the use of comprehensive processes that will ensure systems and data can be recovered with minimal downtime. Strong backup and recovery practices, such as maintaining offline backups and testing whether recovery plans work as intended, can minimize the effects of both disasters and malicious attacks.

Effective data backup and disaster recovery processes are key tools in a Continuity of Operations plan

Continuity of operations planning is becoming more critical as disruptive events and attacks on data and system availability have become more common. Continuity plans set out how an organization will maintain services with minimal disruption in the event of a natural disaster or cyberattack until normal operations can resume. Continuity plans focus on the people and processes needed during a disruption in services, which may include IT resources. This audit looked at how a state agency might address IT systems and data issues within a continuity of operations plan.

A disaster recovery plan focuses on restoring IT systems and data in a timely manner and is an integral piece of a well-designed continuity of operations plan. Most IT systems, to execute a recovery plan effectively, require available backups containing current copies of data and systems that can be restored when the primary data and systems are not operational.

For continuity of operations, state agencies should consider the risks and effects of a disruption of services when developing backup strategies and disaster recovery plans. Agencies should evaluate the effect of impaired data and systems on operations using a business impact analysis, and address issues of risk using an IT risk assessment. They can use the results of the analysis and risk assessment to determine frequency and retention of backups as well as recovery requirements and priorities. The disaster recovery plan specifies the actions needed to recover data, software and IT functionality within a predetermined recovery time. This includes describing how the organization will restore its IT systems from carefully managed backups. These four elements are briefly outlined below.

A business impact analysis helps agencies determine which components of their business activities are most critical to resuming operations. The analysis provides necessary information to develop recovery strategies and make decisions regarding how to allocate resources to ensure operational resilience and continuity of operations during and after a disaster. The analysis should quantify the effects a given type of disaster will likely have on an agency's service delivery; whether limited services are acceptable and for how long; and how quickly an agency can return to normal operations. Once an agency knows what it must do to return to limited or full operations, it can develop strategies, solutions and plans to attain those goals.

An IT risk assessment helps agencies design appropriate strategies and controls to protect their IT systems and data. IT risk assessments are an analysis of potential threats and the likelihood that they will occur. The assessment should document potential threats – including flooding, fire or cyberattack – and how they may affect electronic information, such as

data loss, damage to data integrity, or inaccessible data or systems. Once the potential threats are documented, an agency can score them and decide which risks, to which assets, are high and must be addressed as top priority. Less likely risks, to less valuable assets, might score low and can be dealt with as time and resources permit.

A data backup strategy describes how an agency will make and maintain copies of its data and systems. Agencies should use the results of an IT risk assessment to develop backup strategies that set out which systems or data files should be backed up, how frequently the backup must be performed, where the backup should be stored and for how long. Considerations also include the storage medium – physical media versus cloud-based storage – as well as who in the agency is responsible for managing and testing backup quality. The backup strategy should also spell out how the agency will secure its backups, both physically and electronically.

A disaster recovery plan maps out how an agency will resume its IT-related operations. Agencies should design and test the disaster recovery plan to ensure systems and data can be restored within an acceptable recovery time that is determined by a business impact analysis. The disaster recovery plan should include detailed procedures for recovery, the recovery roles and responsibilities, and contact information of relevant staff. Recovery procedures should be adequately designed to address the threats identified in the IT risk assessment. Among the considerations are whether the disaster is physical – a fire that destroys the worksite and everything stored there, an earthquake that damages a data hub located elsewhere in the region – or a cyberattack that locks or damages essential software. For example, a recovery plan from physical damage might include renting a temporary facility; a plan for cyberattack likely would not.

State requirements and leading practices provide a framework for backup and disaster recovery plans

The Office of the Chief Information Officer (OCIO) has issued a standard and a policy that require state agencies to have data and system backup procedures and a disaster recovery plan. *OCIO Standard 141.10: Securing Information Technology Assets* establishes the state's data backup requirements and *OCIO Policy 151: Information Technology Disaster Recovery Planning* establishes the state's disaster recovery requirements. The standard and policy are discussed in more detail later in this report.

OCIO Standard 141.10 and Policy 151 are available on the OCIO's website: ocio.wa.gov/policies

Leading practices offer guidance about developing comprehensive backup and disaster recovery procedures

To help develop procedures and documentation called for in the OCIO's policies and standards, state agencies may turn to widely available resources and guidance published by both public and private organizations. Some organizations, such as the Center for Internet Security, update their guidance frequently using the latest information about common attack strategies, evolving data storage opportunities, or successful strategies shared by member organizations. Others, including some federal resources, are updated less often but the published standards and manuals include reliable and relevant information for a wide variety of government and business organizations.

Appendix C contains details of state requirements and leading practices related to data backup. **Appendix D** contains requirements and practices related to disaster recovery.

This audit examines whether Washington state agencies could improve their data backup and recovery practices

Earlier audits performed by the Office of the Washington State Auditor have found most agencies generally have data backup procedures, but many lack a current, tested disaster recovery plan and did not regularly perform tests to verify they can restore critical data. Regularly auditing, testing and updating the disaster recovery plan can mean the difference between a fast recovery with minimal impact and days or even weeks of damaging downtime.

This audit examined whether there are adequate backup and disaster recovery policies and procedures in place for selected systems at four state agencies. The audit was conducted to evaluate how closely the four agencies complied with state requirements and aligned with leading practices in these two areas:

- Data and system backups
- Disaster recovery

The selected state requirements and leading practices chosen for our review provide assurance that:

- Data and system backups are secure and available
- A current, tested disaster recovery plan exists that could be used to recover data and systems in the event of a disaster or security incident

Audit Results

Note on reporting protected information

To protect the agencies' IT systems, and the confidential and sensitive information contained in those systems, this report does not include the agencies' names or the detailed descriptions of our results. This information is exempt from public disclosure in accordance with RCW 42.56.420(4). We shared detailed results with each of the audited agencies and with the Office of Cybersecurity at Washington Technology Solutions (WaTech).

While this report does not discuss the specific issues identified during the audit, it does give theoretical examples to provide a general understanding of the types of risks and controls that are involved in data backup and disaster recovery.

Audited agencies can improve their ability to restore critical systems and data in the event of a disaster or security incident

Summary of results

None of the four audited agencies fully and consistently met all state requirements for data backup, disaster recovery, and testing recovery plans. In addition to meeting state requirements, agencies could further reduce disruptions to their services and operations by following the backup and disaster recovery guidance offered by leading practices.

None of the four audited agencies fully and consistently met state requirements for data backup and disaster recovery

All four audited agencies had discrepancies between state requirements and their current practices and procedures. Establishing practices consistent with the state requirements increases an agency's ability to restore data within the agency's expected timeline after a security incident or natural disaster.

To meet state requirements, agency staff must follow the expectations set out in two documents issued by the state's Office of the Chief Information Officer (OCIO). Standard 141.10, section 8.4, concerns data backup, listed in **Exhibit 1**, and discussed further in Appendix C; Policy 151 concerns disaster recovery plans, listed in **Exhibit 2** and discussed in Appendix D. The standards and policy describe at an overview level the actions agencies must undertake. However, each agency must tailor its policies and procedures to its own needs, using tools such as IT risk assessments and business impact analyses.

Exhibit 1 – OCIO Standard 141.10 establishes the state's data backup requirements

An agency must:
• Implement a data backup strategy based on the results of an IT risk assessment
• Implement procedures to periodically test the organization's ability to restore agency data from the backups
• Regularly test the recovery procedures for its critical systems, as described in the agency's IT security program
• Establish methods to secure its backup media
• Store media back-ups in a secure location, such as a designated temporary staging area, an off-site facility, or a commercial storage facility

Source: Office of the Chief Information Officer Standard 141.10.

Exhibit 2 – OCIO Policy 151 establishes the state's disaster recovery requirements

An agency must:
• Develop disaster recovery plans in support of the agency's overall Continuity of Operations Plan
• Consider key things the plan depends on, such as the availability of electricity, communication lines, or other systems
• Update and test the disaster recovery plans at least annually
• Establish methods to secure its backup media
• Document results of tests and planned corrective actions
• Train the appropriate staff so they will be able to execute the disaster recovery plans

Source: Office of the Chief Information Officer Policy 151.

The consequences of failing to address a requirement in either the standard or the policy can be severe. For example, Standard 141.10 calls for backup media to be stored in a secure location. An agency's backup strategy should specify where that location is, or indicate if it will forego physical media and opt for storing data in a cloud environment. Without adequate controls over protecting the backup materials, data could be permanently lost or damaged.

For example, if backups are stored in the same building as the agency's data center – rather than in a secure, off-site facility — a natural disaster that destroys the building will destroy both the primary and backup copies of the data. In this example, data would likely be lost and rebuilt only with considerable effort.

Similarly, failing to adequately tailor the agency's policy or procedures to its own needs and data environment can also lead to problems. For example, Policy 151 includes the instruction to train appropriate staff on the content of the disaster recovery plan. Inadequately trained employees are unlikely to know what to do in the event of a disaster or how to contact key players in the recovery process.

Agencies can reduce disruptions to their services and operations by following backup and disaster recovery guidance offered by leading practices

Leading practices offer guidance about developing backup and disaster recovery procedures that can help state agencies meet the requirements set out by OCIO standards and policies. A state agency that meets only the letter of OCIO requirements for backup and disaster recovery may not develop adequate procedures to recover its data within its predetermined acceptable recovery time. The extra guidance offered by outside resources can help the agency not only meet state requirements but very likely improve its recovery capabilities by taking into account a wider set of considerations.

The three leading resources examined for this audit (see sidebar) offer recommendations and guidance across the topics of data backup and disaster recovery planning. In some cases, their published guidance is no more explicit than materials published by Washington's OCIO. However, in many other cases, the directions they offer are more detailed. For example, OCIO 141.10 requires backup media to be physically secured. Leading practices also suggest all backups have at least one offline copy to protect against a ransomware attack. Increasingly sophisticated malicious attacks make effective backup strategies and disaster recovery plans of vital importance. Following leading practices can help agencies minimize the impact of these costly and often devastating incidents. More information about these leading practices can be found in Appendix C and Appendix D.

Resources for leading practices used in this report

Center for Internet Security (CIS) Critical Security Controls – These controls are designed to help organizations protect their systems and data from known threats.

National Institute of Standards and Technology (NIST) Special Publication 800-34r1 – This publication contains detailed guidelines related to developing backup strategies and disaster recovery plans.

Federal Information System Controls Audit Manual (FISCAM) – This manual presents a methodology for auditing information system controls. It includes control activities related to backup and disaster recovery that are consistent with NIST guidelines.

Leading practices also provide detailed guidance and templates for completing a business impact analysis as part of disaster recovery planning. The business impact analysis provides information needed to develop recovery strategies and make decisions regarding how to allocate resources needed to ensure operational resilience and continuity of operations during and after a disaster. OCIO Policy 151 does not require a business impact analysis; therefore, agencies may not be aware of the value they provide.

State agencies are free to use the advice found in leading practices as they develop their own policies and procedures. The following examples are drawn from the three resources.

Leading practices provide guidance on the frequency, security and testing of data backup systems

Data backup procedures should ensure essential data is backed up regularly; backups are safe from tampering, loss or theft; and that backup systems are tested regularly. To that end, leading practices recommend the organization should take the following actions.

Develop and document backup protocols and procedures, including the frequency and retention of backups. Since many organizations hold data of varying degrees of sensitivity and importance, OCIO requires that they determine backup requirements based on an IT risk assessment that evaluates potential risks of data loss. Leading practices offer more specific guidance, advising that the frequency of backups depends on the volume and timing of the transactions that update data. Systems processing thousands of transactions daily may need to be backed up several times a day, while a system processing a few transactions a day may only need to be backed up weekly. Leading practices further suggest that backup schedules ensure that a recent copy to meet operational needs is always available.

Secure backups against tampering, loss or theft. Organizations should secure their backups against tampering by storing at least one copy offline or otherwise not accessible via a network connection. In addition, they should protect physical backups from loss by placing them in a secured building, which should have fire suppression systems, water sensors and cooling systems to prevent damage to stored materials. Finally, encrypting the backup data in transit and at rest protects confidential data from theft or disclosure to an unauthorized employee or outsider.

Regularly test the organization's ability to restore data. OCIO standards state that agencies must test recovery procedures periodically as determined by the agency's security program. Leading practices specify testing should take place quarterly or whenever the organization purchases new backup equipment. Leading practices also suggest a testing team evaluate a random sample of system backups by attempting to restore them in a test environment. Testers should verify the restored systems to ensure that the restored operating system, applications and data are complete and function properly.

Leading practices also provide guidance on prioritizing, documenting and testing a disaster recovery plan

Having backup copies of the data and systems is just the first step. A state agency must also have procedures in place to ensure that it can recover critical systems and data so it can restore services within a reasonable time. Disaster recovery plans should include a time frame for recovery; elements needed for recovery; and procedures for regular testing. To achieve these goals, leading practices recommend the following tasks for every organization.

Identify recovery priorities and acceptable recovery times. Leading practices recommend the organization perform a business impact analysis to identify the reasonable time to recover, or recovery time objective, and the recovery priorities. When a disaster strikes, resources (including time and staff) are limited. Determining recovery time objectives and priorities in advance takes the guesswork out of recovery to ensure the most critical IT resources are recovered first. The business impact analysis is also used to develop recovery strategies, solutions and plans.

Ensure the plan documents all necessary elements. Examples of elements to record in the plan include:

- Key players, such as security and database administrators, their roles and responsibilities in disaster recovery, and their contact information
- Detailed instructions and procedures on how to restore critical systems and data
- The location of a secondary site and decisions about how it will be staffed

Periodically test and update the plan. OCIO Policy 151 requires state agencies to test disaster recovery plans at least annually, document results of testing, and identify corrective actions based on the results. Leading practices provide further guidance regarding how to test the plan. For example, FISCAM says the most useful testing scenarios involve simulating an actual disaster; a scenario should test whether the alternative data center will function as intended and include restoring systems and data from offsite backups. FISCAM emphasizes that the disaster recovery plan and supporting activities, such as staff training, should be revised to address weaknesses found during testing.

Testing the disaster recovery plan is vital to evaluating whether the plan would be effective in an actual disaster. Because testing the plan – and revising it to correct errors or omissions – is essential, the audit examined this portion of recovery planning in detail.

Three of the four agencies had not performed comprehensive testing of their disaster recovery plans

Comprehensive testing of a disaster recovery plan involves simulating a situation in which the primary data center has been lost. Three of the four audited agencies did not perform comprehensive testing of the disaster recovery plan. One had not tested the plan at all during the past year; the other two tested at some level, but not sufficiently to ensure they could return to full operations. The fourth agency had performed comprehensive testing and developed a corrective action plan for flaws.

Testing can vary in scope, from tabletop exercises, which are discussion-based exercises, to comprehensive testing, which simulates an actual disaster. Tabletop exercises are useful, as they help ensure the key players understand their roles and responsibilities during a recovery situation. However, a tabletop exercise is not a substitute for a comprehensive disaster recovery test, which more rigorously evaluates whether the plan will work. When an agency does not conduct comprehensive disaster recovery tests, the risk of disrupted services and operations can increase significantly.

The purpose of disaster recovery testing is to identify flaws or omissions in the plan so issues can be resolved before an actual disaster or other disruptive event occurs. Examples of flaws or omissions in the plan could include:

- Ineffective procedures, meaning processes that are incorrect or do not account for all the steps needed to achieve the recovery goal
- Outdated procedures, which do not account for new or different data, equipment or staff
- Inappropriate staff assignments – asking people to do things they do not know how to do or have never done before
- Inadequate training – people do not fully understand their role in the recovery process
- Key things the plan depends upon, such as the availability of electricity, communication lines or other systems, may be missing from the plan, decreasing the likelihood of a successful recovery
- Outdated contact information, hampering communications between key staff

Agencies can strengthen their disaster recovery plans by following state requirements and leading practices for testing the plan

OCIO Policy 151 requires agencies to test disaster recovery plans at least annually, document test results, and use them to identify corrective actions and/or risk mitigations. They are further expected to revise their plans to correct the issues tests identified.

Leading practices provide guidance regarding plan testing. Federal Information System Controls Audit Manual (FISCAM) states:

> **"The most useful scenarios involve simulating a disaster situation to test overall service continuity. Such an event would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current."**

National Institute of Standards and Technology (NIST) 800-34 recommends that an organization test each information system component to ensure the effectiveness of the procedures. NIST further recommends the following areas be included in disaster recovery testing:

- Notification procedures
- System recovery on an alternate platform from backup media
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations

Audited agencies lacked the resources and guidance they needed to establish comprehensive backup and disaster recovery practices and procedures

Summary of result

Executive managers at some agencies were not always aware of the risks and potential consequences and did not always allocate adequate resources to address the risks. We found none of the four audited agencies adequately used IT risk assessments and business impact analyses to identify and inform management of the risks. Executive management's investment in technology and staff is nonetheless key to implementing effective backup strategies and disaster recovery plans. Better statewide guidance and tools could help agencies implement more effective backup strategies and disaster recovery plans.

Executive managers at some agencies were not always aware of all risks and potential consequences, and so did not always allocate adequate resources to address the risks

None of the four audited agencies adequately used IT risk assessments and business impact analyses to identify and inform management of the risks

Agency leaders and executive management need current, accurate information that includes a complete picture of the risks and consequences presented by security incidents and natural disasters. In addition, they need to understand the costs of implementing an effective backup and disaster recovery program. With such information in hand, they can prioritize where the limited resources of their agency are most needed to address the risks and needs of the agency, and ensure the effort is adequately funded. Two key tools help provide this kind of critical information to management: IT risk assessments, which help agencies identify threats, and business impact analyses, which help them prioritize their key functions. However, none of the audited agencies used IT risk assessments to develop their data backup strategies, and none of them had up-to-date business impact analyses.

Staff at one audited agency said that deficiencies in backup and disaster recovery programs could arise when management lacks knowledge of the risks and consequences of inadequate planning. In some cases, audited agencies were unaware of some risks and thought their processes were adequate.

Executive management's investment in technology and staff is key to implementing effective backup strategies and disaster recovery plans

Implementing and maintaining an effective backup strategy and disaster recovery plan requires a significant investment in technology and staff. The investment is not merely a one-off expenditure. One auditee observed that funding must be ongoing if it is to adequately support successful backup and disaster recovery efforts in the long term. Technology investments recur because both hardware and software tools constantly change and improve. Investments in employees ensure they are adequately trained to perform disaster recovery processes specific to an agency.

Two of the four audited agencies did not always make maintaining the disaster recovery plan a priority

Some audited agencies did not have a designated person who was responsible for maintaining the disaster recovery plan. For example, one audited agency had assigned a full time employee to manage disaster recovery for the selected system. When that person retired, the agency did not fill the position but instead distributed the responsibilities between four employees, who took on the disaster recovery tasks along with their current job duties. This reduction in resources poses two kinds of problems. It creates a challenge for staff to effectively manage the disaster recovery program while performing their other primary responsibilities, and management will have more difficulty ensuring all aspects of the program receive adequate attention. Another agency did not assign an employee to maintain the plan for the selected system.

One audited agency attributes their backup and disaster recovery program's success to support from executive management

When executive managers actively engage with backup and disaster recovery efforts and support these activities, their agencies can more effectively address and mitigate risks. For example, IT staff at an agency that had implemented many state requirements and leading practices said their executive managers supported the disaster recovery program and dedicated staff to testing and maintaining the plan. Other factors staff said contributed to the success of the program:

- Having well-documented procedures in place to recover data and systems
- Using standard templates that are easy to update and maintain
- Separating parts of the disaster recovery plan into separate documents for ease of reviewing and updating, which also makes them easy to use during disaster recovery exercises

Finally, the agency also comprehensively tests the disaster recovery plan at least once a year, and documents and tracks any gaps discovered through testing in a corrective action plan. Agency staff attributed their success to the maturity of their disaster recovery program, employees who are dedicated to maintaining the disaster recovery plan, and support from executive management.

Better statewide guidance and tools could help agencies implement more effective backup strategies and disaster recovery plans

Our audit results show that state agencies could benefit from additional guidance regarding available backup solutions. The OCIO does not issue specific guidance concerning data backup strategies to accompany Standard 141.10. Helpful guidance could include suggestions for testing backups and up-to-date options for protecting backups from sophisticated malicious attacks.

The need is just as great for improving disaster recovery plans. Successful disaster recovery planning is likely to be a tremendous undertaking. OCIO Policy 151, in summary, instructs agencies to do the following:

- Develop a disaster recovery plan considering dependencies
- Test the plan and document results and corrective actions
- Update the plan at least annually
- Train appropriate staff on contents of the plan and how to execute it

However, the policy does not give state agencies guidance on how to develop a comprehensive disaster recovery plan or how to test the plan to ensure it is effective. Further guidance and tools, including templates and examples, could be helpful to agencies in developing a disaster recovery program that will prepare agencies for recovering from a variety of events.

The OCIO has published a document titled *IT Disaster Recovery and Business Resumption Guidelines*. However, these guidelines were last updated April 2002, more than 18 years ago, and therefore do not realistically reflect the current IT environment. Furthermore, the guidelines were not listed on the OCIO policies, procedures and guidelines webpage: we found them using the search function on the OCIO website. For these guidelines to be useful, they should be updated to reflect changes to technology and current risk environment and be easily accessible to state agencies.

State Auditor's Conclusions

State agencies' ability to provide essential services relies heavily on the availability of a variety of IT systems. Any number of things can happen to interrupt the availability of those systems, including relatively mundane equipment failures, unforeseen natural disasters, or malicious security attacks. When these events happen, it is important for agencies to have reliable backups of their systems and their data, as well as a solid plan to recover their most important systems quickly.

The state's security requirements and other sources of leading practices can help agencies develop effective backup and disaster recovery plans that are tailored to the business needs and risks each agency faces. In the appendices of this report, we have compiled those requirements and leading practices in one place. These are important resources, and we would encourage all state agencies to take advantage of them as they develop their own recovery plans.

Recommendations

For the audited agencies

To reduce the risk of not being able to restore critical systems and data in the event of a disaster or malicious attack, we recommend the following:

1. Agencies perform and use IT risk assessments and business impact analyses to identify gaps in current backup and disaster recovery practices and procedures, recovery time objectives, and recovery priorities.
2. Executive management consider the results of these analyses and work closely with IT staff to ensure adequate resources are allocated to design and implement comprehensive backup and disaster recovery practices and procedures.
3. Agencies further align backup and disaster recovery practices and procedures with state requirements and leading practices.

For the Office of the Chief Information Officer

To improve the ability of state agencies to comply with Standard 141.10 concerning data backup and Policy 151 concerning disaster recovery planning, we recommend the OCIO:

4. Update the IT Disaster Recovery and Business Resumption Guidelines and make them readily available to state agencies via the ocio.wa.gov website.
5. Offer agencies tools and templates for backup strategies and disaster recovery planning, such as IT Risk Assessments and Business Impact Analyses.

Guidance for all state agencies

We consider the audit results so broadly applicable that it is in the state's best interest for every state agency to undertake the actions communicated to the few that participated directly in the audit. We therefore suggest all Washington state agencies consider the recommendations made to the audited agencies as they develop and implement their backup and disaster recovery programs. In addition, we suggest they apply leading practices from publications such as:

- CIS Critical Security Controls
- NIST 800-34
- FISCAM – Contingency Planning

Appendices C and D in this report contain links to state requirements and resources for leading practices related to backup and disaster recovery.

Agencies could also refer to the #BeCyberSmart section of the State Auditor's Office website for additional resources. It contains a set of curated resources we have compiled on various cybersecurity issues. Though these resources are intended to assist local governments with cybersecurity, state agencies may also find some of them helpful, in particular the Backup and Recovery Best Practices brochure.

Agency Response

JAY INSLEE
Governor

JAMES WEAVER
Director &
State Chief Information Officer

STATE OF WASHINGTON
WASHINGTON TECHNOLOGY SOLUTIONS
Washington's Consolidated Technology Services Agency
1500 Jefferson Street SE ▪ Olympia, Washington 98504-1501

September 15, 2020

The Honorable Pat McCarthy
Washington State Auditor
P.O. Box 40021
Olympia, WA 98504-0021

Dear Auditor McCarthy:

On behalf of the audited agencies, thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report, "Data Backup and Disaster Recovery."

We appreciate the information provided and the recommendations to improve and strengthen data backup and disaster recovery processes.

Effective data backup and disaster recovery processes are key tools in a Continuity of Operations plan. We agree that there is opportunity to strengthen processes and commit to doing so. Updated guidance and tools from my office can help agencies assess their disaster recovery plans and backup processes. As technology evolves, we all must continually review and update guidance, plans and processes to determine risks and ensure continuity of essential services to Washingtonians.

The audited agencies value the SAO's recommendation to align backup and disaster recovery practices further with state requirements and leading practices. Leading practices may offer guidance that can help state agencies meet the requirements set by my office. We also appreciate the report recognizing that,

> *"Implementing and maintaining an effective backup strategy and disaster recovery plan requires a significant investment in technology and staff. The investment is not merely a one-off expenditure…Technology investments recur because both hardware and software tools constantly change and improve. Investments in employees ensure they are adequately trained to perform disaster recovery processes specific to an agency."*

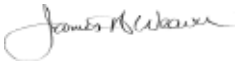
In the current economic climate initiated by the global pandemic, state agencies may lack funding and resources. We recognize that we must elevate the need to invest in resources

required to close gaps in these processes and staffing. We believe that with support from my office and collaboration among state agencies we can make significant progress toward strengthening backup and disaster recovery programs.

We appreciate the time your staff spent working with my office and the selected agencies to look for improvements. We would like to compliment the auditors. They were professional, knowledgeable and engaged. Please thank your team for their collaborative work.

As always, we continue to welcome the SAO's observations and recommendations.

Sincerely,



James Weaver
Director & State Chief Information Officer

cc: David Postman, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Keith Phillips, Director of Policy, Office of the Governor
David Schumacher, Director, Office of Financial Management
Christine Bezanson, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
Vinod Brahmapuram, State Chief Information Security Officer, Washington Technology Solutions
Scott Bream, State Information Policy Officer, Washington Technology Solutions
Scott Frank, Director of Performance Audit, Office of the Washington State Auditor

Official State Cabinet Agency Response to the Performance Audit on Data backup and Disaster Recovery – 2020, Sept. 15, 2020

The State's Chief Information Officer on behalf of the audited agencies provides this management response to the State Auditor's Office (SAO) performance audit report received Aug. 13, 2020.

SAO Performance Audit Objectives:

The SAO sought to answer these questions:

1. Have selected state agencies implemented data and system backup policies and procedures that comply with state requirements and align with leading practices?
2. Do the selected state agencies have a current, tested, disaster recovery plan that complies with state requirements and aligns with leading practices?

SAO Recommendations to the four selected state agencies: To reduce the risk of not being able to restore critical systems and data in the event of a disaster or malicious attack, we recommend the following:

1. Agencies perform and use IT risk assessments and business impact analyses to identify gaps in current backup and disaster recovery practices and procedures, recovery time objectives, and recovery priorities.
2. Executive management consider the results of these analyses and work closely with IT staff to ensure adequate resources are allocated to design and implement comprehensive backup and disaster recovery practices and procedures.
3. Agencies further align backup and disaster recovery practices and procedures with state requirements and leading practices.

STATE RESPONSE: We agree with the opportunities for improvement identified by the SAO and will continue to work diligently to remediate the issues identified. We are committed to ongoing assessment and improvement of backup and disaster recovery programs, as well as constructive communication and collaboration between agencies and those providing guidance and policy. Agencies need clear direction and timelines to effectively plan, improve and ensure resources as technologies evolve.

Where feasible, we will further align data backup and disaster recovery processes with the leading practices recommended in the CIS Controls, NIST Special Publication, and FISCAM.

The following action steps in response to the performance audit recommendations will support efforts to improve and maintain our data backup and disaster recovery plans.

Action Steps and Time Frame

- Audited agencies will establish a cadence for reviewing state requirements and leading practices and improving alignment where feasible. *By December 31, 2020.*
- Agencies will coordinate and gather business unit and technical interdependencies to conduct a business impact analyses through the Interagency Continuity of Operations Planning (iCOOP) Committee, beginning March 1, 2021. We estimate this process to take up to a year. *By March 31, 2022*.
- Audited agencies will conduct an IT risk assessment and business impact analyses. *By March 30, 2022*.
- Audited agencies' executive management (after completion and analysis of the IT Risk Assessment) will consider the results, risks, and resources assigned toward design, implementation and improvement of comprehensive backup routines. *By October 31, 2022.*
- Audited agencies' executive management (after completion and analysis of the IT Risk Assessment) will consider the results, risks, and resources assigned toward design, implementation and improvement of comprehensive disaster recovery routines. *By October 31, 2022.*

SAO Recommendations to the Office of the Chief Information Officer: To improve the ability of state agencies to comply with Standard 141.10 concerning data backup and Policy 151 concerning disaster recovery planning, we recommend the OCIO:

4. Update the IT Disaster Recovery and Business Resumption Guidelines and make them readily available to state agencies via the ocio.wa.gov website.
5. Offer agencies tools and templates for backup strategies and disaster recovery planning, such as IT Risk Assessments and Business Impact Analyses.

STATE RESPONSE: The OCIO agrees with the opportunities for improvement identified by the SAO and will work with other stakeholders to update guidelines and identify tools and templates to better assist agencies. The OCIO will coordinate with the Emergency Management Division of the Military Department who, through the iCOOP, is responsible for disseminating Continuity of Operations Planning (COOP) guidance to state agencies on methods of aligning to standards.

Action Steps and Time Frame

- OCIO will convene a workgroup with Military Department, Office of Cybersecurity (OCS), OCIO and agency Subject Matter Experts (SMEs) to evaluate updates to guidelines and identification of tools and templates. *By September 30, 2021*.
- The OCIO with the assistance of the workgroup will publish guidelines, tools and templates. B*y March 31, 2022*.

Appendix A: Initiative 900 and Auditing Standards

Initiative 900 requirements

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to U.S. Government Accountability Office government auditing standards.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Results and Recommendations sections of this report.

I-900 element	Addressed in the audit
1. Identify cost savings	**No.** The audit does not identify cost savings. The purpose of this audit is to ensure there are current and effective back up and disaster recovery plans in place.
2. Identify services that can be reduced or eliminated	**No.** Data and system backup and disaster recovery processes are critical to government operations and this audit does not evaluate whether they can be reduced or eliminated.
3. Identify programs or services that can be transferred to the private sector	**No.** Data and system backup and disaster recovery processes are critical to government operations and this audit does not evaluate whether they can be transferred to the private sector.
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** The audit compares backup and disaster recovery processes and procedures against state requirements and leading practices, and makes recommendations to align them.
5. Assess feasibility of pooling information technology systems within the department	**No.** The audit reviews various government systems and agencies to determine the effectiveness of their back up processes and disaster recovery plans. It does not evaluate the feasibility of pooling technological systems.

I-900 element	Addressed in the audit
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**No.** The audit does not analyze departmental roles and functions, nor provide recommendations to change or eliminate them.
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** Statutory or regulatory changes are not necessary to implement the audit's recommendations.
8. Analyze departmental performance data, performance measures and self-assessment systems	**No.** The audit identifies gaps in the audited agencies' back up and disaster recovery procedures. We did not analyze agency's performance data, performance measures or self-assessment systems.
9. Identify relevant best practices	**Yes.** The audit identifies and uses leading practices maintained by the Office of the Chief Information Officer, the Center for Internet Security, National Institute of Standards and Technology, and the United States Government Accountability Office. See Appendices C and D.

Compliance with generally accepted government auditing standards

We conducted this performance audit under the authority of state law (RCW 43.09.470), approved as Initiative 900 by Washington voters in 2005, and in accordance with generally accepted government auditing standards as published in Government Auditing Standards (December 2011 revision) issued by the U.S. Government Accountability Office. 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.

The mission of the Office of the Washington State Auditor

To provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective. The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic subscription service. We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program. For more information about the State Auditor's Office, visit www.sao.wa.gov.

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email *Webmaster@sao.wa.gov* for more information.

Appendix B: Scope, Objectives and Methodology

Scope

The audit reviewed a total of four systems at four state agencies. Systems were selected based on several factors, including how critical it is to the agency's mission and how much state residents rely on it. The results of the audit are specific to the systems, not the agencies or the state as a whole.

The audit assessed the extent to which agency backup strategies and disaster recovery processes align with selected state requirements and leading practices. The requirements and practices chosen for our review provide assurance:

- Data and system backups are secure and available
- A current, tested disaster recovery plan exists that could be used to recover data and systems in the event of a disaster or security incident

Objectives

The objective of this performance audit was to examine how closely the four selected agencies complied with state requirements and aligned with leading practices in these two areas:

- Data and system backups
- Disaster recovery

Methodology

We obtained the evidence used to support the findings, conclusions and recommendations in this audit report during our fieldwork period (June 2019 to May 2020), with some additional follow-up work afterward. We summarize the work we performed to address each of the audit objectives in the following sections.

Objective 1: Examined how closely the four selected agencies complied with state requirements and aligned with leading practices related to data and system backups

To address this audit objective, we gained an understanding of auditee data and system backup policies and procedures for the selected systems by analyzing documents and conducting staff interviews. In particular, we looked for evidence that each auditee properly secured backups and performed test restoration of data and systems. We compared our observations to state requirements and leading practices and identified key areas for improvement.

Objective 2: Examined how closely the four selected agencies complied with state requirements and aligned with leading practices related to disaster recovery

To address this objective, we gained an understanding of auditee disaster recovery policies and procedures for the selected systems by analyzing documents and conducting staff interviews. In particular, we looked for evidence that each auditee performed disaster recovery testing, including corrective action plans based on test results. We compared our observations to state requirements and leading practices and identified key areas for improvement.

Work on internal controls

This was an audit of internal controls over disaster recovery and back up plans. We reviewed controls that provide assurance:

- Backup data is protected
- Backup data is restorable
- A comprehensive, effective disaster recovery plan is documented and tested
- The plan is current and approved and based on a business impact analysis
- Errors and issues with recovery from the secondary site are identified and corrected

Our audit looked to see if these controls were adequately designed and followed. Our audit did not look at controls over the completeness and accuracy of data and system backups.

Reporting confidential or sensitive information

Because public distribution of tests performed and test results could increase the risk to the state, the public audit report does not present details of our work. We gave specific, detailed recommendations to the four agencies to implement procedures and update disaster recovery plans that follow state requirements and leading practices.

Appendix C: State Requirements and Leading Practices: Data backup

State agencies are required to comply with Washington State Office of the Chief Information Officer (OCIO) policies and standards. Agencies can also use leading practices as guidance for creating effective backup strategies and disaster recovery processes to protect against data loss and system downtime. This appendix presents key requirements and examples of leading practices relating to backup policies and procedures. See Appendix D for information directly related to disaster recovery plans.

State requirements

OCIO *Standard 141.10: Securing Information Technology Assets, Section 8.4*. This standard lists general requirements over data and systems backups, such as:

- Implement a data backup strategy based on the results of an IT risk assessment
- Implement procedures to periodically test the organization's ability to restore agency data from the backups
- Regularly test the recovery procedures for critical systems, as described in the agency's IT security program
- Establish methods to secure backup media
- Store media back-ups in a secure location such as a designated temporary staging area, an off-site facility, or a commercial storage facility

Leading practices

Center for Internet Security, Critical Security Controls V.7.1, *Control #10: Data Recovery Capabilities*. Control #10 is a best practice covering operating system, application and data backup and recovery. Control #10 consists of five sub-controls that state agencies should consider implementing to ensure the data is complete and available in the event data and/or systems need to be restored. (See **Figure 1** on the following page for a list of the sub-controls).

In addition, Control #10 provides extra guidance by recommending "Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional."

Figure 1 – Recommended practices from Control 10: Data Recovery Capabilities

Sub-control	Action to take
10.1: Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.
10.2: Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
10.3: Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
10.4: Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
10.5: Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

Source: Center for Internet Security Controls V. 7.1.

NIST Special Publication 800-34 3.4.2 and section 3.5 of FISCAM, published by the United States Government Accountability Office (GAO), provide additional guidance for implementing effective backup processes and procedures. Backup topics covered by NIST and FISCAM include:

- Policies for frequency and scope of backups
- Offsite storage
- Accessibility of backup data
- Security
- Structural and environmental conditions of storage facility

Data backup online resources

OCIO Standard 141.10: Security Information Technology Assets, Section 8.4.
ocio.wa.gov/policy/securing-information-technology-assets-standards

CIS Center for Internet Security CIS Control 10. cisecurity.org/controls/data-recovery-capability/

NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems.
nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Federal Information System Controls Audit Manual (FISCAM). gao.gov/assets/80/77142.pdf

Appendix D: State Requirements and Leading Practices: Disaster recovery

State agencies are required to comply with Washington State Office of the Chief Information Officer (OCIO) policies and standards. Agencies can also use leading practices as guidance for creating effective backup strategies and disaster recovery processes to protect against data loss and system downtime. This appendix presents key requirements and examples of leading practices relating to disaster recovery planning, policies and procedures. See Appendix C for information directly related to data backup policies and procedures.

State requirements

OCIO *Policy 151: Information Technology Disaster Recovery Planning*. This standard lists general requirements over disaster recovery planning, such as:

- Develop disaster recovery plans in support of the agency's overall Continuity of Operations Plan
- Consider key things the plan depends on, such as the availability of electricity, communication lines and other systems
- Update and test the disaster recovery plans at least annually
- Document results of tests and planned corrective actions
- Train the appropriate staff so they will be able to execute the disaster recovery plans

Leading practices

As with data and system backups, NIST and FISCAM provide additional guidance regarding disaster recovery planning. NIST 800-34, Rev. 1 (2010), *Contingency Planning Guide for Federal Information Systems*, Chapter 3, lays out the steps in the disaster recovery planning process. Each step of the process is followed by detailed guidance how to accomplish each step. See **Figure 2** for recommended steps.

FISCAM Critical Element CP-3 complements NIST guidance by providing a thorough list of control techniques for developing and documenting a comprehensive disaster recovery plan. FISCAM Critical Element CP-4 provides control techniques for testing the plan and updating it as appropriate.

Figure 2 – Steps in the disaster recovery planning process based on NIST guidance

1.	Develop contingency planning policy
2.	Conduct the business impact analysis
3.	Identify preventative controls
4.	Create contingency strategies
5.	Develop an information system disaster recovery plan
6.	Plan testing, training, and exercises
7.	Plan maintenance

Source: Auditor developed from NIST 800-34, Rev. 1 (2010), Contingency Planning Guide for Federal Information Systems.

By aligning backup and disaster recovery procedures with state requirements and leading practices, state agencies can minimize disruption and loss resulting from natural disasters and security incidents.

Disaster recovery online resources

OCIO Policy 151: Information Technology Disaster Recovery Planning.
ocio.wa.gov/policy/information-technology-disaster-recovery-planning

NIST Special Publication 800-34 Rev. 1 *Contingency Planning Guide for Federal Information Systems*.
nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Federal Information System Controls Audit Manual (FISCAM). **gao.gov/assets/80/77142.pdf**

"Our vision is to increase **trust** in government. We are the public's window into how tax money is spent."

– Pat McCarthy, State Auditor

Washington State Auditor's Office
P.O. Box 40031 Olympia WA 98504

www.sao.wa.gov

1-564-999-0950

Office of the Washington State Auditor