Chief Operations Office (COO)
Chief Procurement Office (CPO)

# DCS Vendor Management and Performance

## Internal Audit Report 17-101

January 2018

Department of Information Resources

## Internal Audit Mission Statement

To collaborate with DIR leadership to fulfill the agency's core mission by providing independent and objective audit services designed to add value and improve the effectiveness of risk management, control, and governance processes.

## DIR Internal Audit Staff

Lissette Nadal, CIA, CISA, CRISC, Director

Cathy Sherwood, CPA, CITP, CISA, CTCM, Audit Project Manager

Megan Hudson, CISA, Senior Auditor/ Contractor

# Table of Contents

# Executive Summary

This report summarizes the scope, results, and recommendations from the work performed in conducting the Data Center Services (DCS) Vendor Management and Performance audit. This performance audit was included in the approved Fiscal Year 2017 Internal Audit Annual Plan.

The **audit objective** was to determine whether DCS reported vendor performance complied with established Service Level Agreements (SLAs).

To accomplish the audit objective, the audit team reviewed 12 months of SLA performance measures and assessed whether supporting documentation for activities or events included in selected SLA measures were aligned with contractual Functional Requirements Document (FRDs). Internal Audit examined relevant documentation to help determine whether reported performance measures from Atos, the DCS service component provider (SCP) selected for review, provided evidence of compliance with established SLAs. The audit team reviewed applicable criteria, including the DCS Service Management Manual (SMM), State of Texas Service Level Guide, Service Level Agreement FRDs, and related procedure documents and work instructions, management reports prepared by the Multi-Sourcing Services Integrator (MSI), and published enterprise compliance reports. In conducting our audit procedures, we interviewed DCS subject matter experts, including staff from the MSI Service Performance and Reporting (SP&R) team.

The audit **scope** included performance metrics from the DIR contract with Atos based on the project risk assessment results. The following reported performance metrics (SLAs for server, data center, network, and mainframe) were selected for additional testing based on the risk approach applied, and for the period from October 2015 through September 2017:

- Incident Resolution Time
- CMDB Reconciliation
- License and Maintenance Renewal Timeliness
- Successful Backups
- Successful Recoveries
- Change Management Effectiveness
- Disaster Recovery Test Plan Objectives Met
- Disaster Recovery Test Report

Overall, reported vendor performance complied with established SLAs. Although Internal Audit noted some data entry errors and differences between reported measures and updated measures in the online performance reporting system, DIR's control environment includes ongoing communication among the contractor groups, internal DIR governance, and the DCS customers that served to resolve any error and discrepancies identified. Performance reports

are maintained on a Collaboration Portal where stakeholders can obtain real time information about SLAs, and the status of incident tickets, work orders, service requests, and change requests.

Based on the results of the audit work performed, reported performance complied with contract provisions, as defined in the SLA FRDs for the Atos contract. Because the MSI relies on data from Atos that is compiled using both automated and manual processes before information is uploaded into the SLA compliance reporting tool[1], additional periodic review of Atos' internal processes surrounding the collection of information would enable DIR to gain additional assurance about the integrity and reliability of reported performance data. Recommendations to management included:

- Restrict changes to source documents that have been closed in the Collaboration Portal – Information Technology Service Management (ITSM) System to prevent erroneous errors in reported performance metrics.
- Expand the responsibility for approval or rejection of SLA exception requests to include participation from both the Chief Procurement Office (CPO) and the Chief Operations Office (COO) with a panel of at least three DIR representatives.
- Develop additional documentation for (a) mainframe backup reporting processes, and (b) a backup schedule for systems that were part of the transition from the previous DCS vendor.
- Retain support for the Change Management Effectiveness SLA performance measure, including documented reconciliations between completed CRQs from the Remedy Ticketing System and monthly final enterprise compliance reports.
- Improve outreach efforts and reporting to continue engaging DIR customers to (a) assist with maintaining an accurate and complete CMDB, and (b) increase disaster recovery testing of their critical applications.

DIR management from the DIR CPO, and COO Operations concurred with the results and recommendations reported by Internal Audit and provided action plans, estimated completion dates, and assigned responsibility to management staff for implementing the recommendations.

We conducted this performance audit in conformance with the *International Standards for the Professional Practice of Internal Auditing* and in accordance with the *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 issues and

[1] DCS Collaboration Portal in ServiceFlow is the SLA reporting compliance tool.

conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our issues and conclusions based on our audit objectives.

Internal Audit thanks management and staff from the DIR CPO, COO Operations, and the MSI for their time, cooperation, and assistance provided during this assurance audit.

Detailed results of the audit are documented in the report that follows.

# Background

In December 2011, DIR executed three multi-year contracts to provide consolidated Data Center Services (DCS) to 28 state agencies and Angelo State University. The first contract was awarded to Capgemini North America, Inc., to act as a Multi-Sourcing Integrator (MSI) enabling the State of Texas to standardize processes and maximize the value of its Information Technology (IT) services. The six-year contract, with an initial value of approximately $127 million, included service level management, service desk support, project management, IT security, business continuity, disaster recovery, and financial management.

The second contract was signed with ACS State and Local Services, Inc., a wholly-owned subsidiary of Xerox Corporation, to provide infrastructure services in four areas: mainframe, servers, networks, and data center operations. Atos acquired Xerox State and Local Services in June 2015. The eight-year contract, with an initial value of approximately $1.1 billion, emphasized delivering improved customer services, stabilizing the State's IT infrastructure environment, and consolidating computer servers from legacy agency data centers to the state's two consolidated data centers.

The third contract was awarded to Xerox Corporation to provide bulk printing and mailing services. The six-year contract, with an initial value of approximately $56 million, leverages the state's significant mail volumes to keep costs low, while providing more flexibility to state agencies to meet their business needs.

Atos, the Service Component Provider (SCP) selected for review as part of this audit based on the risk assessment results, provides participating state agencies and other publicly funded entities with technology infrastructure that supports important Texas programs such as: the supplemental nutrition assistance program, unemployment insurance, and child support. The SCP assists with operating legacy agency data centers while consolidating operations to two modern facilities. By consolidating from an aging, disparate infrastructure spread across approximately 1500 locations and 31 data centers, the state continues to upgrade technology to realize the vision of shared services. The objectives of the DCS include:

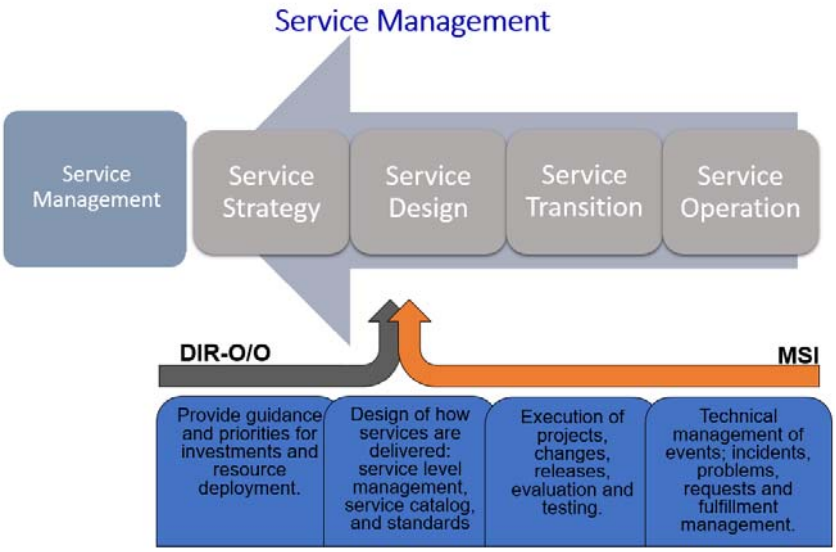
- Enable Texas state agencies to access data center computing as a managed service, share costly data center infrastructure, reduce focus on IT operations, and concentrate on their core business.
- Provide mainframe, server, network, data center, and print-mail services.

The focus of this audit was on the Atos Master Services Agreement. However, some recommendations were directed to the Multi-Sourcing Services Integrator (MSI) in their role in managing the service level performance process. See the audit objective and scope in Appendix A.

**Description of Service Level Agreements (SLAs)**

The Service Level Agreements (SLAs) are an important part of the Atos Master Services Agreement (MSA), the Contract. The SLAs include qualitative measures for services provided as well as quantitative descriptions and reporting obligations that should be met by the DCS contractors. Established SLAs define services to be delivered, service level targets, and key responsibilities of the service component providers, DIR, and the MSI.

Critical service level metrics and key measures for DCS components are defined by the contract. The MSI is responsible for collecting information from DCS SCPs, including Atos. Most SLA data flows via automatic feed from the DCS ITSM tool (Remedy) to an SLA management and reporting system (ServiceFlow) maintained by the MSI. In instances where there is no automatic connection, SCPs provide SLA measurement data via flat file for validation and upload to the SLA reporting tool. Both automated and manual processes are in place to collect information that is used to track SLA compliance. The diagram below shows the coordination between DIR and the MSI with respect to service management.




This audit project was included in the Fiscal Year 2017 Internal Audit Annual Plan to determine whether the DCS reported vendor performance comply with established SLAs **(audit objective)**. The scope of this audit included performance metrics selected based on risk for the period from October 2015 through September 2017:

- Resolution Time
- CMDB Reconciliation
- License and Maintenance Renewal Timeliness
- Successful Backups (server and mainframe)
- Successful Recoveries (server and mainframe)

- Change Management Effectiveness
- Disaster Recovery Test Report Delivery
- Disaster Recovery Test Plan Objectives Met

Additional details on the **Scope and Methodology** of this audit are documented in Appendix A of this report.

# Detailed Results

Overall, reported vendor performance complied with established service level agreements (SLAs). Although Internal Audit noted some data entry errors and differences between reported measures and updated measures in the online performance reporting system, DIR's control environment includes ongoing communication among the contractor groups, internal DIR governance, and the data center services (DCS) customers served to resolve any error and discrepancies identified. Reports are maintained on a Collaboration Portal where stakeholders can obtain real time information about SLAs, and the status of incident tickets, work orders, service requests, and change requests.

DIR actively monitors SLAs at the enterprise level and meets frequently with the Atos service component provider, customers, and MSI to address performance issues needing improvement. Performance issues identified are shared with the Service Delivery Solutions Group[2] (SDSG) and formal reports are presented summarizing performance results. In addition, DIR Customer Service Operations (CSO) utilizes a monthly scorecard to obtain ongoing feedback from the DCS customers on the service component provider's performance. Performance results are communicated to DIR executive leadership and governance boards, and summary reports are presented at DIR Board meetings.

Based on the results of the audit work performed, reported performance complied with contract provisions, as defined in the SLA functional requirements documents (FRDs) for the Atos contract. Because the MSI relies on data from Atos that is compiled using both automated and manual processes before it is uploaded into the DCS Collaboration Portal – ServiceFlow, the SLA compliance reporting tool, additional review of Atos' internal processes surrounding the collection of information would enable DIR to gain additional assurance about the integrity and reliability of reported performance data. Recommendations to management included:

- Restrict changes to source documents that have been closed in the Collaboration Portal – Information Technology Service Management (ITSM) System to prevent erroneous errors in reported performance metrics.
- Expand the responsibility for approval or rejection of SLA exception requests to include participation from both the Chief Procurement Office (CPO), and Chief Operations Office (COO) with a panel of at least three DIR representatives.
- Develop additional documentation for (a) mainframe backup reporting processes, and (b) a backup schedule for systems that were part of the transition from the previous DCS vendor.

[2] The **Service Delivery Solutions Group** is one of DIR's governance groups made up of representatives from DIR, the Service Component Providers, and the MSI and provides a point of escalation for vendor performance issues.

- Retain support for the Change Management Effectiveness SLA performance measure, including documented reconciliations between completed CRQs from the Remedy Ticketing System and monthly final enterprise compliance reports.
- Improve outreach efforts and reporting to continue engaging DIR customers to (a) assist with maintaining an accurate and complete CMDB, and (b) increase disaster recovery testing of their critical applications.

Details are described in the issues and recommendations that follow.

# Issue 1: Changes to Closed Remedy Tickets

Closed Remedy[3] tickets (CRQs) were changed after being counted for final Service Level Agreement (SLA) compliance reports. Restricting changes once closed helps establish data integrity within the Remedy Ticketing System and ensures output consistency for standard management reports. Changes should not be made to Remedy tickets after the tickets are closed and included in a final Enterprise Compliance Report.

Software License and Renewal SLA – Key Dates

The ***"Requested End Date"*** corresponds with the expiration date for software license and hardware maintenance contracts.

The ***"Actual End Date"*** is the date used to assess whether Software License Renewal SLAs were met or not met.

The ***"Completed Date"*** is the date license and renewal activities are completed and were typically shortly before the closed date.

The ***"Closed Date"*** is the date when all tasks associated with a CRQ are finalized for SLA purposes.

Remedy tickets that have been closed may inadvertently be updated after SLA required compliance reports are finalized. The DCS staff indicated that "closed" isn't necessarily a permanent status and that in some instances, tickets may be re-opened.

In September 2016, the "Change Management Effectiveness" SLA for the server tower was included in the final Enterprise Compliance Report as 97.04%, which is slightly below the contractor's expected performance level of 97.08%. The reported result on the final Enterprise Compliance Report was correct; however, the reported service level reflected in a live data inquiry from ServiceFlow by auditors resulted in 97.17%, a difference of .0013%. When the audit team requested an explanation for the change in SLA performance results, the MSI staff indicated that (a) a ticket was inadvertently updated which impacted the historical September 2016 SLA results as displayed in the online reporting tool and (b) the correct SLA percentage should have not changed from the reported result of 97.04%.

Changes to Remedy tickets that impact ServiceFlow data made after final compliance reports are published can negatively affect data integrity for source records and increases the potential that misstatement of current or future reported performance results based on data feeds from source systems will be undetected.

[3] The **Remedy Ticketing System** is part of the IT Service Management module in the DCS Collaboration Portal. It is a tool used for initiating, working, and closing service desk tickets, including change requests (CRQ's), incident tickets (INC's), work orders (WO's), and other types of service delivery tickets.

**Recommendation:**

The DIR Chief Operations Office (COO) management should:

A. Restrict user access to prevent changes to closed tickets from the Remedy Ticketing System, and require a new ticket if corrections are needed after a ticket has been closed.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendation.*

*The action plan, estimated completion date, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 2: Closed Change Requests with No Completed Date

Closed software license and maintenance renewal change requests (CRQ's)[4] did not always include a populated "completed date". For license and renewal activities, the "closed date" is the date when all tasks associated with the CRQ have been closed, and the "completed date" is the date license and renewal activities are completed. The Service Management Manual (SMM[5]) procedures require that the status be "closed" to be measured in the Service Level Agreement (SLA). However, based on the published SMM, "closing the CRQ is a validation step and does not drive the SLA."

Atos creates a CRQ to address renewals and installs for all software license and hardware maintenance agreements scheduled to expire. Upon ticket creation, the Service Component Provider (SCP) populates the "requested end date" with the expiration date for software license or hardware maintenance contracts. The "actual end date" is auto-populated by IT Service Management (ITSM) when all tasks associated with the CRQ have been closed, and the renewal activities must be completed prior to installation.

Although the software license renewal SLA is driven by the comparison of the "actual end date" and the "requested end date" from the CRQ, the date that license and renewal activities were completed is not always reflected in the "completed date" for the CRQ. Once the CRQ has auto-

[4] A **change request** is an electronic Remedy record describing changes requested to the infrastructure, including LANS, network, backup systems, storage devices, Servers, applications, or any appliance or other component associated with or potentially impacting any part of the DCS contract, including data center building maintenance.

[5] The creation of a **Remedy CRQ** with all required information is used to facilitate the software renewal process. The CRQ documents the DCS customer approval and tracks the software renewal through completion. At this time, a draft contract module record is created and related to the expiring contract module record by the service provider. SMM PRO-419-01 states that closing the CRQ is a validation step and does not drive the SLA. Once the CRQ has auto-completed, it is routed to the MSI for final review and closing. The MSI will close the CRQ.

completed, it will return to the MSI Change Management Team for final review and closing. Then, the MSI Change Management Team closes the CRQ.

The audit team reviewed twenty-seven (27) completed and closed change tickets for software license renewals (CRQs) from the September 2016 final Enterprise Compliance Report and noted:

- Twelve (12) "closed" change tickets had "completed dates" populated shortly after the "actual end date", and
- Fifteen (15) "closed" change tickets did not include an entry in the "completed date" field.

For one of the CRQs closed without a "completed date", the missing date resulted from a DIR customer that improperly re-opened the CRQ, causing the "completed date" to automatically reset to a null value in the ITSM. When a member of the MSI Tools Team reset the change status back to "closed", the "completed date" field did not auto-populate. As of September 2017, the "completed date" field remained blank.

In another example, the CRQ status was changed to "pended" without a business reason documented in the ticket notes. The CRQ was included in the September 2016 Enterprise Compliance Report. However, the "completed date" for the CRQ was in October 2016. According to the MSI, closing a CRQ is a validation step and does not drive the SLA. During the audit, the MSI change managers revised the CRQ status to "closed" and updated the "completed date" field.

The MSI Service Performance and Reporting Group is responsible for reviewing and validating the reported data while not being directly engaged in operations. When the status of a completed CRQ is changed to from "closed" to "pending", and the original "completed date" is automatically cleared because of this action, data integrity issues and unauthorized changes to CRQs could go undetected.

**Recommendation:**

The DIR Chief Operations Office (COO) management should:

A. Coordinate with the Multi-Sourcing Integrator (MSI) to ensure that all "closed" CRQs have a populated "completed date" with accurate information, as required by Service Level Agreement (SLA) functional requirements documents, and as part of the MSI's review process, before the measures are calculated and included in the Enterprise Compliance Report.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendation.*

*The action plan, estimated completion date, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 3: Monitoring Contractor Performance

Service level exceptions "by Service Level Agreement (SLA)" and "by DIR customer" are not periodically summarized and reported to the DIR Chief Procurement Office (CPO), the Division responsible for contract management, and DIR does not have a management dashboard to efficiently report on service performance issues, including details about the root cause and resolution of recurring service level exceptions. The State of Texas Comptroller of Public Accounts (CPA) issues guidance and training for contract managers across the state and states that one responsibility of a Contract Manager is to monitor the contractor's progress and performance to ensure goods and services conform to the contract requirements.

Coordination and communication between DIR's operations and procurement staff about the results of SLA measurement, including approvals for exceptions, is needed to ensure contract managers maintain required contractor performance records, documentation of significant events, and the contractor's progress and performance is properly monitored. Refer to Appendix B for a complete list of the Contract Manager responsibilities, as defined by the CPA's guidance. In addition, management reports summarizing approved SLA exceptions can help ensure contract managers take action to introduce and execute needed changes to contract provisions timely or develop a Service Level Improvement Process, if needed.

Trends in SLA exceptions by "cause of breach" and the impact on reported vendor performance measures support DIR business decisions, including future amendments to SLAs or other contract provisions. DIR operations management indicated that exception trend reports (a) have previously been provided to the Service Delivery Solutions Group (SDSG) as part of that governance group's monthly SLA review, (b) could also be provided to the CPO, and (c) are available on an ad-hoc basis.

Detailed examples of SLA exceptions requested by either the SCP or the MSI approved by the DIR operations staff were shared with COO and CPO management to support the recommendation to change from a one-person approval process to establishing a three-panel group to approve or reject requested SLA exceptions. Exception details are included in MSI Service Performance and Reporting management reports and are discussed during weekly SLA Exception Meetings.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Establish a formal method of communicating Service Level Agreement (SLA) issues to contract management staff and include representation from the Chief Procurement Office (CPO) on a panel of at least three individuals authorized to approve or reject SLA exception requests.

B. Develop a RACI Chart[6] with defined areas of responsibility and accountability between CPO Contract Management and COO Operations staff for SLA performance management.

C. Develop and implement a shared contract and operations management dashboard to report on the categorization of SLA exceptions accepted.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 4: Management of SLA Targets

Changes to Service Level Agreement (SLA) targets were made before amendments to the contract were formally executed or a contract change request (CCR) was approved in the Salesforce System by all required parties. SLA targets are defined to establish the expected performance level for each SLA. These are updated and approved operationally before contract amendments are executed which is allowed by the Data Center Services (DCS) contract. The DCS contract allows SLAs to be updated by administrative change and without formal amendment if they are being updated in accordance with requirements in Exhibit 3. SLA performance levels are revised annually as part of the contract continuous improvement process and supporting documentation for contract documents and approvals are documented in the Salesforce System.

The *Comptroller of Public Accounts Contract Management Guide* suggests that changes to service levels are subject to written approval, documentation, and a bilateral agreement.

Approvals are obtained through CCRs and later memorialized in contract amendments. Updates to SLA targets should be approved at least 30 days before they become effective by all three parties involved (DIR, MSI, and Atos). However, approval for contract changes that became effective in July 2016 were not formally approved until August 2016 for the MSI and January 2017 for the Service Component Provider, and formal contract amendments had not been executed for these updated SLA targets.

The CPA Contract Management Guide suggests that these types of changes are subject to written approval, documentation, and a bilateral agreement. When CCRs are used to modify

[6] A **RACI Chart** illustrates the different levels of responsibility within the various teams. RACI tables show who is Responsible, Accountable, Consulted and Informed for each procedural step.

expected performance levels, contract management staff must track these agreements to ensure they are not overlooked when developing future contract amendments.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Develop a process to standardize legal agreements (bilateral agreements) specific to annual updates to service level performance targets to ensure updates are memorialized in a contract amendment, as required.

B. Ensure contract change requests for updates to service level performance targets are documented in the Salesforce System and approved timely by all required parties.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 5: Disaster Recovery Test Plan and Schedule

Upon review of the "Disaster Recovery Test Plan Objectives" SLA, the audit team noted less than 20 percent of the total "Class 1" and "Class P" applications eligible for annual disaster recovery testing, as classified in the configuration management database (CMDB), were included in the approved fiscal year 2016 Disaster Recovery Exercise Test Plan and Schedule. Appendix 21 – Exhibit 16 of the contract with the Service Component Provider– states that "for all applications designated as having "Class P" and "Class 1" RTO's (Recovery Time Objectives), the SCP shall perform annual DR tests, except where directed otherwise by DIR and DIR customers, and will complete the initial DR test within twelve (12) months." During fiscal year 2016, only 13 of 18 customers with eligible applications, tested eligible applications. The remaining five customers did not test any of their eligible applications. The MSI reported that only 31% of eligible "Class 1" applications were tested in fiscal year 2016.

Based on the current approach, DIR offers disaster recovery testing services, and DIR customers have the option to request testing for their critical systems. DIR management does not believe it is feasible to test all critical systems for every customer each year, but that additional outreach to DIR customers could help increase the awareness and utilization of available DR testing services.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Develop a process to document and retain DIR customers' approval or rejection to schedule Disaster Recovery (DR) tests for eligible "Class 1" and "Class P" applications in IT Service Management Remedy tickets.

B. Report to the IT Leadership Committee (ITLC) annually the "Class 1" and "Class P" applications not tested, by customer.

C. Ensure all eligible "Class 1" and "Class P" applications from the CMDB are included in the fiscal year test plan and schedule before approval. If customers or DIR approve an exception for testing, document the decision on the official schedule based on information available at the time the annual schedule is prepared for DIR approval.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 6: Disaster Recovery Test Report Timeliness

Upon review of the "Disaster Recovery (DR) Test Report Delivery" Service Level Agreement (SLA), the audit team noted there is no system date and time stamp to validate that disaster recovery test reports are delivered timely. The SLA, "DR Test Report Delivery" measures the percentage of time the SCP delivers DR test reports within 30 calendar days of the scheduled DR test. A DR test report is deemed as not delivered timely if a DR test is not completed as scheduled or is not scheduled. However, the contracted Functional Requirements Document (FRD) allows the exclusion of events if approved by DIR through the SLA exception procedure documented in the Service Management Manual (SMM). According to DIR management, final reports are not required to be formally accepted and approved by DIR or its customers. Two draft test reports were included in the DCS Collaboration Portal as final reports and counted for both corresponding SLA performance targets. In both instances, the final reports were delivered 32 calendar days late based on the date the reports were posted to the portal.

According to the DR Exercise Process, Procedure (PRO) 412-03 of the SMM, DIR customer approval in written format is not required for their DR test results posted in the DCS Collaboration Portal. However, the formal approval would serve as evidence of communication and acceptance of (a) test results, (b) additional corrective actions, and (c) potential changes to established Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) targets.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Implement a process to allow the DIR customers to formally approve the test results included in their final disaster recovery test reports.

B. Implement a process for independent validation of the completed date and time for disaster recovery test reports posted in the DCS Collaboration Portal and used for Service Level Agreement (SLA) measures.

C. Update the Functional Requirements Document (FRD) to include posting draft and final test reports in the DCS Collaboration Portal for SLA performance target purposes.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 7: Server Backup Failure Processes

### Backup Failure Reporting

Server backup failure processes are defined in the Service Management Manual (SMM) in Procedure PRO-801-05, Backup Failure Reporting Process. As part of the reporting process, inconsistencies in the "Outcome" and "Service Level Agreement (SLA) Success" fields within the Backup11 Report were noted. For three of thirty (30) server backup failures reviewed, backup failures were not resolved timely or the resolution of the closed ticket was not documented in the Remedy ticket. Backup11 reports are detailed reports from Bocada. Due to size limitations, only the summary Backup11 report can be uploaded into the DCS Collaboration Portal – ServiceFlow, a subset of the same report which is used to calculate SLA results. The MSI validates that the data in the Backup11 reported matches data in ServiceFlow.

### Backup Failure Procedures

Per the SLA, the Service Component Provider (SCP) is required to provide a Backup11 Report every month showing the results of the backups for each customer, and an enterprise report showing the backup results for all DIR customers. The audit team reviewed a sample of 30 server backup failures from the Backup11 Report for the month of August 2017. These backup failures impacted two DIR customers and were due to:

- Backup Timeout Errors (13 backup failures),
- Backup Software Errors (5 backup failures),
- Backup Unknown Errors (2 backup failures), and
- Multiple errors at once (10 backup failures).

Of the 30 failures, 25 were rerun the same day and resulted in successful backups. Reruns are appropriate when backup failures occur. However, the remaining five backup failures resulted in the following observations:

- Inconsistent results in the "Outcome" and "SLA Success" fields of the Backup11 Report (2 failures). These should have reported the same information in the "Outcome" and "SLA Success" columns.
- The auditor sampled the same backup job on two consecutive days. A successful rerun of a backup failure from 8/4/17 and another on 8/5/17 were not completed until 8/15/2017. The Incident Ticket that was issued did not note a resolution of the issue that caused the failure (1 backup, two days of failure). The ticket should have been resolved and the notes should specify the resolution.
- One backup failure on 8/12/2017, did not have a successful rerun until 8/19/2017. The Incident Ticket was created a day later than what the procedures (PRO-801-05)[7] specify and was closed as 'successful' before a successful backup was completed (1 backup failure). Backup failures should be investigated, and a ticket should be created after three consecutive backups have failed without a successful rerun. Tickets should not be closed as "successful" until resolution is reached, and the backup is successful.

The backup failure process is not being consistently followed, as specified in the contracted procedures, and some failures are not truly resolved. If issues are not resolved in a timely manner and the reports do not accurately represent the outcome of the backup, critical customer data may not be backed up or recovered by the SCP. Management communicated that backup scheduling and related configuration settings for the customers' managed applications are the customers' responsibility. The SCP, Atos, is responsible for completing the backups and reporting any failures, successes, and re-runs to the MSI's Applications Management Team. The SCP uses the Avamar tool to backup virtual environments, remote offices, enterprise applications, and network-attached storage (NAS) servers. In addition, the SCP uses the Bocada backup reporting tool to generate the flat files required to be loaded to the DCS Collaboration Portal – ServiceFlow for service level management and reporting purposes. The MSI uses the logic from the Functional Requirements Document (FRD) for backup SLAs to validate the flat file data loaded to the portal by the SCP, conducts compliance assessments, and includes the results of the assessments in the DCS Collaboration Portal.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

[7] According to PRO-801-05, "out of window backups" are successful backups that ran outside of the established backup window; they are counted as a failure with regards to SLA reporting, but are not considered as a failed backup for incident management.

A. Ensure backup failures follow the specified Backup Failure Reporting process, as described in the established procedures PRO-801-05.

B. Ensure issues related to backup failures are resolved and resolved timely with complete documentation in the incident tickets.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 8: Mainframe Backup Process and SLA Reporting

The Service Level Agreement (SLA) for "Successful Backups for Mainframes" describes the methodology the Service Component Provider (SCP), Atos, should follow to backup DIR customer specified files on the mainframe. The SCP reports the results to the Multi-Sourcing Integrator (MSI) by loading a flat file to the DCS Collaboration Portal-ServiceFlow. However, Atos did not provide sufficient documentation describing mainframe backup scheduling, backup, and reporting processes. The SCP is responsible for documenting the processes in place to backup servers and mainframes. The MSI is responsible for ensuring this documentation is up-to-date, and available to the customers through the DCS Collaboration Portal.

The audit team met with the Atos Mainframe Backup Team to gain an understanding of the processes in place for documenting mainframe backup schedules and results and requested supporting documentation for 1) the actual processes in place, and 2) testing the effectiveness of the "Successful Backups for Mainframes" SLA. Although the SCP indicated that updates and changes to the mainframe backup schedule are requested, tracked, and implemented in accordance with the standard DCS service request process, the audit team could not perform testing in this area due to inadequate process documentation. Specifically, a schedule for mainframe backups is not retained by Atos and a log of completed mainframe backups was not available for review. Because the SCP assumed responsibilities from the previous DCS SCP in 2015, they have continued to run backups that were already established for mainframes with little or no documentation about backup scheduling.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Ensure the Service Component Provider (SCP) documents the process in place to implement and accomplish the methodology described in the "Successful Backups – Mainframe" SLA Functional Requirements Document (FRD).

B. Approve the mainframe backup process documented by the SCP.

C. Ensure the Multi-Sourcing Integrator (MSI) posts the SCP's approved mainframe backup process documentation in the DCS Collaboration Portal.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 9: Change Request (CRQ) Count Reconciliations

The audit team reviewed the Functional Requirements Document (FRD) for the "Change Management Effectiveness" Service Level Agreement (SLA) and reperformed steps to validate results for the February 2017 and May 2017 Final Enterprise Compliance Report results. The service level calculation for "Change Management Effectiveness" is the number of changes that are successfully implemented by the Service Component Provider (SCP), divided by the number of changes implemented by the SCP. Examples of changes that are not successfully implemented include those that cause a severe incident, are backed out or the time to implement exceeded the agreed upon measurement window. For purposes of change management effectiveness, changes are reported in the measurement window when the change ticket is "closed". Change tickets are closed after all implementation activities (i.e., tasks) associated with the change have been closed, and after all required DIR or DIR customer approvals have been obtained.

The audit team generated a list of all change requests (CRQs) from the Remedy Ticketing System for the months of February 2017 and May 2017 and noted discrepancies between the count of CRQs meeting the criteria described in the "Change Management Effectiveness SLA" FRD and the count of CRQs included in the monthly Enterprise Compliance Report from the DCS Collaboration Portal – Service Flow. We noted that the logic for compiling data for this SLA includes specific types of changes and excludes those related to software license and hardware maintenance agreements. There are specific change types, such as "asset maintenance" and "project" changes that are not included in the "Change Management Effectiveness" SLA.

When final SLA compliance results are reported monthly, a reconciliation of (a) weekly to monthly counts in ServiceFlow, and (b) ServiceFlow monthly counts to the monthly counts included in the Information Technology Service Management (ITSM) – Remedy Ticketing System would provide assurance that the counts in the final monthly compliance reports are an accurate representation of CRQs completed during the period. In addition to the counts, the reconciliation should include a variance explanation of any differences identified. Because data updated in the ITSM – Remedy can affect the results included in the ServiceFlow reports, identifying differences is needed to ensure that the final Enterprise Compliance Report results can be reperformed and verified.

The COSO Framework, an internal controls framework, suggests that ongoing monitoring procedures include regular management and supervisory activities, peer comparisons and trend analysis using internal and external data, reconciliations, and other routine actions. Documentation of reconciliations should be maintained to provide additional assurance that CRQs are included, or excluded, in according with the "Change Management Effectiveness" SLA.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Require the MSI to reconcile the change request (CRQ) counts from the DCS Collaboration Portal-ServiceFlow to the CRQ counts from the ITSM-Remedy Ticketing System, and to the final published Enterprise Compliance Report.

B. Retain documentation of (a) reconciliations performed in the DCS Collaboration Portal, and (b) the reconciliation process in the Service Management Manual (SMM).

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 10: CMDB Reconciliation SLAs

The DCS configuration management database (CMDB) is used to store configuration records throughout their lifecycle, including attributes of hardware and other configuration items (CIs). The audit team reviewed the "CMDB Reconciliation" Service Level Agreement (SLA) for the month of August 2016 and noted the reported performance complied with the methodology, as described in the SLA for CMDB reconciliation. DIR management continues to streamline the process to manage the CMDB using automated tools to capture information about the state IT assets. DIR management anticipates that the transition to a more automated process will improve the Service Component Provider (SCP)'s ability to track and manage the IT assets inventoried in the CMDB.

The following table summarizes the (1) count of mainframe, data center, network, and server assets in the CMDB, (2) count of CMDB records that met or did not meet SLA requirements, and (3) number of SLA exceptions approved. Overall, the SCP met SLA targets and the auto-discovery tool is responsible for detecting over 95 percent of the assets in the CMDB.

| Description | Mainframe | Data Center | Network | Server | Totals |
|---|---|---|---|---|---|
| Unique CMDB Serial Numbers | 29 | 65 | 167 | 5,572 | 5,833 |
| SLA Met | 26 | 37 | 129 | 5,557 | 5,749 |
| SLA Not Met | 3 | 28 | 38 | 15 | 84 |
| Number of SLA Exceptions Approved | 3 | 26 | 38 | - | 67 |
| | | | | | |
| Percent of Exceptions Submitted and Approved | 100.0% | 92.9% | 100.0% | N/A | 79.8% |
| Percent of "SLA Not Met" Records | 10.3% | 43.1% | 22.8% | 0.3% | 1.4% |

To assess the reasons for documented SLA exceptions associated with updates to the CMDB, the audit team judgmentally selected work orders for 35 asset updates from the detailed CMDB reconciliation worksheets for the mainframe, data center, and network service towers. The audit team compared the CMDB reconciliation details with the corresponding work order details and noted that (a) two assets were excluded from SLA measurement because the MSI was not able to read the serial numbers when the physical inspection was performed, and (b) a work orders were created to correct 12 asset records from “SLA Not Met” to “SLA Met” based on a physical inspection at one of the data centers during the CMDB reconciliation process. Based on the corresponding work order, three (3) network configuration items were not at the data center, and it was determined that the status for these configuration items needed to be changed to “disposed”.

For the server CMDB reconciliation, there were no SLA exceptions noted. An automated tool is currently used to scan the DIR network to identify server assets, and key fields identified by the server tool are compared to the CMDB data. If assets not included in the CMDB are identified, the counts are included in the denominator for the SLA calculation and categorized as “SLA Not Met” events.

Although the automated process is helping management continuously improve the CMDB accuracy, the SCP is no longer required to report on the CMDB reconciliation SLAs for the mainframe, network, data center, and print-mail assets. DIR management indicated that although these SCP assets are no longer included in specific SLAs, they continue to be subject to operational reporting and improvement initiatives. Because the CMDB serves as the source for many DCS billable services, the audit team recommended that periodic inspection of assets be part of an established measurement for the SCP’s performance in maintaining an accurate and complete CMDB.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Establish new Service Level Agreement (SLA) for CMDB accuracy and data quality for all service towers as part of the next Multi-Sourcing Integrator (MSI) contract.

B. Continue to involve customers in identifying assets that should be included in the CMDB and in documenting resolution of discrepancies noted, based on the results of reconciliations performed.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 11: Backup SLA Data Integrity

The Service Level Agreement (SLA) for "Successful Backups – Mainframe" and "Successful Backups – Servers" measures the number of times the Service Component Provider (SCP) completes backup jobs successfully and within the specified timeframes during the applicable measurement window divided by the number of times the SCP should have completed backup jobs within the applicable measurement window, with the result expressed as a percentage.

Based on this methodology and as documented in the contractual Functional Requirements Document (FRD), a SLA Tracking Spreadsheet (saved as a flat file) is uploaded into the DCS Collaboration Portal – ServiceFlow only including jobs that have been completed. This prevents any "null" fields from being uploaded into ServiceFlow. The Multi-Sourcing Integrator (MSI) is responsible for collecting the source data before it is provided to the customer. This methodology provides for the opportunity for the MSI to potentially manipulate the source data to show high percentage outcomes. Because the source data must be manually adjusted prior to reporting for service level outcomes, the process for collecting supporting data should be reviewed at the SCP level to assess the reliability and validity of the reported data.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Require the Service Component Provider (SCP) to develop and document procedures for collecting the source data used for Service Level Agreement (SLA) performance reporting on successful backups.

B. Approve the Service Component Provider's documented data collection process for SLA performance reporting.

C. Ensure the MSI posts the SCP's approved data collection process documentation in the DCS Collaboration Portal.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 12: Update Backup Functional Requirements Document

The Functional Requirements Document (FRD) for backups states that "timeframes for backup executions are maintained in the Service Management Manual (SMM) by the Service Component Provider (SCP), to include the Schedule, Retention-periods and Target (SRT) directories". SRTs are created by the DIR customer and used as the backup schedule for customer data. However, timeframes for customer backup executions are maintained in individual SRT documents on the DCS Collaboration Portal and not as part of the SMM, as currently documented in the FRD. DIR management confirmed that the reference in the FRD is incorrect, and the timeframes are maintained and should be maintained in the SRT document and not in the SMM. The FRD does reference the SRTs; however, this reference should be clarified to accurately represent the location of SRTs.

**Recommendation:**

The DIR Chief Operations Office (COO) should:

A. Update the Functional Requirements Document (FRD) to accurately describe where the timeframes for DIR customer backup executions should be maintained.

***Management Response:***

*DIR management from the COO agreed with Internal Audit's recommendation.*

*The action plan, estimated completion date, and responsible DIR management staff are documented in Appendix D of this report.*

## Issue 13: Work Order Status for Successful Recoveries

The work order statuses reviewed did not always reflect successful recoveries accurately. The contracted Functional Requirements Document (FRD) for the "Successful Recoveries" Service Level Agreement (SLA) defines the process for determining service levels for successful recoveries. Successful recoveries are defined as "the total number of service requests for data recovery that are initiated successfully and within the specified timeframes during the applicable measurement window, divided by the total number of service requests for data recovery that were scheduled to be initiated during the applicable measurement window, with the result expressed as a percentage."

The audit team reviewed the SLA for "Successful Recoveries" for mainframes and servers and generated a list of all work orders submitted during the month of June 2017 for two DIR customers. The audit team noted two work orders were closed with a status of "Successful with Issues" and the notes did not show resolution (see detail below). The audit team inquired about

closing work orders as “Successful with Issues” with no documentation on how the issues were resolved. The Multi-Sourcing Integrator (MSI) indicated that the recoveries completion procedures allow for recoveries that did not result in a successful restore to be closed as "Successful with Issues” because work was performed to recover data. In the auditors’ opinion, this practice does not accurately represent the results of the work as the restore itself was not successfully completed.

In addition, we noted the following two issues with the work orders reviewed:

- A closed work order with a status of "Successful with Issues". The work order notes state that the restore was unsuccessful and the information was recreated manually. The MSI indicated that the assigned resolver completed the Work Order with “Status Reason=Successful with Issues” because work was performed with issues in completing a specific aspect of the work order. Involvement from the requester was required for directory permissions.

- Another example included a work order that was closed with a status of "Successful with Issues”. However, the notes state that the restore was not successfully completed. The MSI indicated that work orders are being “completed not resolved”. The request could not be fulfilled, and the resolver was unable to schedule initiation of data recovery because the folder in the specified “File Folder Location” did not exist. The resolver performed research and notified the requester of the findings, then placed the Work Order into “Status=Completed” and “Status Reason=Successful with Issues” as work was performed.

Because the methodology for measuring “Successful Recoveries” indicates recoveries that are initiated successfully are counted for SLA reporting purposes, there is opportunity for inaccurate representation on the resolution of data recovery issues. Closing a work order as successful, if the issue was not resolved, does not accurately represent the state of the issue and allows for issues to go unresolved but shown as meeting the SLA performance target. In the audit team’s opinion, adding additional statuses for data recovery issues such as “unsuccessful, but complete”, “customer approved and unsuccessful”, or “customer approved and canceled” may help DIR management isolate recurring issues and develop appropriate corrective actions. Some of the recurring issues noted by the audit team included:

- Issues related to contractor staff errors,

- DIR customer-related issues, and

- Inability to locate the target data requested for restore.

**Recommendations:**

The DIR Chief Operations Office (COO) should:

A. Require the Multi-Sourcing Integrator (MSI) to update the successful recovery procedures to ensure work order statuses accurately represent the results of data restorations and revise the Service Level Agreement (SLA) methodology accordingly.

B. Revise the SLA reporting methodology to allow for the work orders closed with a status of “Successful with Issues” to include an additional level of detail that summarizes the types and/or cause of issues encountered when attempting to restore DIR customer data.

***Management Response:***

*DIR management from the COO agreed with Internal Audit’s recommendations.*

*The action plans, estimated completion dates, and responsible DIR management staff are documented in Appendix D of this report.*

# Appendix A: Objectives, Scope, and Methodology

The audit **objective** was to determine whether Data Center Services (DCS) reported vendor performance complied with established Service Level Agreements (SLAs).

The audit **scope** included performance metrics from the DIR contract with Atos, Service Component Provider. The following reported performance metrics (SLAs for server, data center, network, and mainframe) were selected for additional testing based on a risk-based approach, and for the period from October 2015 through September 2017:

1. Resolution Time (server, network, data center, mainframe) – measures the percentage of time Service Component Provider resolves incidents within the applicable timeframes. If an incident is escalated, then the resolution time clock restarts upon escalation. Upon escalation, a new ticket will be created, and the original ticket will be cancelled. The cancelled ticket will be related to the new ticket.

2. CMDB Reconciliation (server, network, data center, mainframe) – measures the percentage of a random sample of inventory records that is determined to be accurate.

3. License and Maintenance Renewal Timeliness (server) – measures the timeliness of software license and hardware maintenance renewals and installs managed by the SCP. Expirations for software license and hardware maintenance are maintained in the Multi-Sourcing Integrator (MSI) Contract Management Module.

4. Successful Backups (server, mainframe) – measures the percentage of time SCP completes backup executions on systems successfully during the applicable Measurement Window in accordance with the relevant criteria for the schedule, retention-periods, and target directories.

5. Successful Recoveries (server, mainframe) – measures the percentage of time the SCP initiates data recoveries within the specified timeframe during the applicable measurement window. Specific target timeframes for each service tier are specified in the contract.

6. Change Management Effectiveness (server, data center, network, mainframe) – measures the percentage of time the SCP successfully implements changes.

7. Disaster Recovery Test Report Delivery (server, data center, network, mainframe) – measures delivery of disaster recovery test reports within 30 calendar days of the scheduled disaster recovery test. The Disaster Recovery Test Schedule is documented by the SCP in the annual DR Test Plan, and may be modified prior to the test, per the rescheduling procedure maintained in the Service Management Manual (SMM).

8. Disaster Recovery Test Plan Objectives Met (server, data center, network, mainframe) – measures the percentage of time Service Component Provider(s) successfully tests, as defined in the Service Management Manual (SMM), DCS customer and SCP

infrastructure. If a test is unsuccessful, the SCP must remediate and successfully re-perform any failed test within ninety (90) days following the initially scheduled test (or such longer period as may be agreed upon by the Parties). The measurement is calculated based on successfully completing the overall test objective, which must be defined before the test. For purposes of clarity, note that an objective may be met successfully even if issues are identified, provided that the overall objective is met.

The following areas were excluded from the scope of this audit project:

1. Availability (server, data center, mainframe, network, semi-managed servers),
2. Service request fulfillment (server, data center, network, mainframe),
3. Solution proposal delivery (server, data center, network, mainframe),
4. Solution implementation (server, data center, network, mainframe),
5. Invoice dispute resolution (server, data center, network, mainframe),
6. Root cause analysis (server, data center, network, mainframe),
7. Corrective actions (server, data center, network, mainframe),
8. Offsite media management (server, data center), and
9. Batch processing completed within window (mainframe).

The audit **methodology** included:

- Interviews with subject matter experts involved with DCS service level management.
- Review of a sample of SLA performance measures to determine whether:
    - Reported measures included all required contract elements.
    - Reported measures were mathematically accurate with service level credits and earn backs properly assessed.
    - SLA exceptions applied to the measure were properly authorized by DIR.
    - Automated or manual processes used in collecting measurement data aligned with and supported accurate performance reporting.
- Review of supporting documentation for activity or events included in the SLA measure aligned with the related Functional Requirements Document (FRDs) describing the methodologies for the SLA measures, the logic used in the calculations, source documents required, datasets used in the measure, exclusions, data collection procedures, subject matter experts, and queries with specific field names addressing the elements included in the SLA measurements.

- Review of relevant documentation such as the SMM, and State of Texas Service Level Guide, compliance reports, and other policies and procedures.
- Data analysis to evaluate 12 months of performance data.
- Review of the Final Enterprise Compliance Report to evaluate performance trends and remediation for instances when the Service Component Provider, Atos, did not meet established service levels.

Audit **criteria** used in the performance of this audit included:

- Texas Government Code,
- Texas Administrative Code,
- State of Texas Comptroller of Public Accounts – Contract Management Guide,
- Atos contract and contract amendments, attachments, and exhibits,
- DIR's Enterprise Contract Management Plan,
- DCS State of Texas Service Level Guide,
- DCS Service Management Manual, and
- Other documented policies and procedures.

# Appendix B: Contract Managers' Responsibilities

Contract Manager's responsibilities relevant to oversight of service level agreements are bolded in the list below. The Contract Management Guide published by the State of Texas Comptroller of Public Accounts (CMG-CPA) defines the primary Contract Manager responsibilities to include:

- Participating in developing the solicitation and writing the draft documents. Contract administration must be considered during this process.
- **Consulting with legal counsel to address any legal concerns and/or issues.**
- **During solicitation development determine if the contractor's compensation structure is appropriate for the work.**
- **Serving as the point of contact for disseminating the instructions regarding the work to the contractor/ vendor.**
- Receiving and responding to communications between the agency and the contractor.
- Managing, approving, and documenting any changes to the contract.
- Managing any state property used in contract performance, e.g., computers, telephones, identification badges, etc.
- **Identify and resolve disputes with contractor in a timely manner.**
- Implementing a quality control/ assurance process.
- **Maintaining appropriate records.**
- **Documenting significant events.**
- **Monitoring the contractor's progress and performance to ensure goods and services conform to the contract requirements.**
- **Exercising state remedies, as appropriate, when a contractor's performance is deficient.**
- Inspecting and approving the final product/ services by submitting a written document accepting the deliverables.
- Monitoring the budgeting/ accounting process to ensure sufficient funds are available.
- Verify accuracy of invoices and authorize payments consistent with the contract terms.
- Performing contract closeout process ensuring the contract file contains all necessary contract documentation, formal acceptance documented, and document lessons learned.

# Appendix C: Glossary

The glossary provides key terms referenced in the audit report. Definitions were obtained from the master services agreement, state rules and regulations, ITIL® and other relevant guidance or professional standards.

**Change Request (CRQ)** – A change request an electronic Remedy record describing changes requested to the infrastructure, including LANS, Network, backup systems, storage devices, servers, applications, or any appliance or other component associated with or potentially impacting any part of the data center services (DCS) contract, including data center building maintenance.

**Configuration Management Database (CMDB)** – A database used to store configuration records throughout their lifecycle. The configuration management system maintains one or more configuration management databases, and each database stores attributes of configuration items, and relationships with other configuration items.

**Final Enterprise Compliance Report** – Monthly management report that summarize service level performance, due to DIR by the 20th calendar day of each month following the reporting month. The report is compiled and reported using data from the DCS Collaboration Portal – ServiceFlow.

**IT Infrastructure** – All hardware, software, networks, facilities etc. that are required to develop, test, deliver, monitor, control or support applications and IT services. The term includes all information technology but not the associated people, processes, and documentation.

**Measurement Window** – The measurement window is the defined time period stated in each Functional Requirements Document (FRD) applicable to SLA measures.

**Multi-Sourcing Integrator (MSI)** – The MSI acts to standardize processes and to provide service delivery management, service desk support, project management, disaster recovery, and financial management services. The MSI coordinates DCS for mainframes, servers, networks, print and mail, and data center operations provided by multiple service component providers.

**Recovery Point Objective (RPO)** – RPO is the maximum targeted period in which data might be lost from an IT service due to a major incident. (loss of data)

**Recovery Time Objective (RTO)** – RTO is the amount of time the business can be without the service, without incurring significant risks or significant losses. (loss of IT service)

**Remedy** – An IT Service Management module in the DCS Collaboration Portal used for initiating, working, and closing service desk tickets, including change requests (CRQ's), incident tickets (INC's), work orders (WO's), and other types of service delivery tickets.

**ServiceFlow** – The DCS Service Level Reporting System that receives data from automatic or manual data feeds used by the MSI in validating performance results and publishing monthly SLA performance compliance reports.

**Service Management Manual** – Service Component Providers execute SLA measurements in accordance with processes and procedures in the Service Management Manual, a virtual management policy and procedure manual for the delivery of data center services. The manual references Functional Requirement Documents (FRDs) that are also available in the DCS Collaboration Portal.

**SLA Exceptions** – Exceptions that are authorized by DIR management for SLA items that do not meet measurement standards but have a valid reason for being excluded.

**SLA Validation** – Service Level validation procedures describe the high-level steps for daily, weekly, and monthly monitoring, and validation of Service Level data, including critical and key measures. Members of the MSI Service Performance and Reporting team monitors Service Levels, identify Service Level issues, and work with the appropriate teams to remediate. Service Component Providers also monitor and validate SLA performance and contact the MSI to discuss reporting issues.

**Verification and Audit** – The activities responsible for ensuring that information in the CMDB is accurate and valid, and that all configuration items have been identified and recorded. Verification includes routine checks that are part of other processes – for example, verifying the serial number of a desktop PC when a user logs an incident. Audit is a periodic, formal check.

# Appendix D: Recommendations and Management Responses

| Recommendation[8] | Management Response | | |
|---|---|---|---|
| | Action Plan[9] | Estimated Implementation Date[10] | Responsible Management Staff[11] |
| **Issue 1: Changes to Closed Remedy Tickets** | | | |
| A. Restrict user access to prevent changes to closed tickets from the Remedy Ticketing System, and require a new ticket if corrections are needed after a ticket has been closed. | DIR management will work with the MSI to restrict ticket updates for closed Remedy tickets. | 9/1/18 | Director, Operations, Chief Operations Office (COO) |
| **Issue 2: Support for SLA Performance Data** | | | |
| A. Coordinate with the Multi-Sourcing Integrator (MSI) to ensure that all "closed" CRQs have a populated "completed date" with accurate information, as required by Service Level Agreement (SLA) functional requirements documents, and as part of the MSI's review process, before the measures are calculated and included in the Enterprise Compliance Report. | DIR management will work with MSI as part of the SLA compliance assessment process to update SLA validation processes to confirm that CRQs coded for "Change Management Effectiveness" and "License and Maintenance Renewal Timeliness" SLA measurement to have all data fields populated in accordance with corresponding SLA functional requirements documentation at the time of the validation and before DIR review and approval of the monthly enterprise SLA compliance report. | 4/1/18 | Director, Operations, COO |
| **Issue 3: Monitoring Contractor Performance** | | | |
| A. Establish a formal method of communicating Service Level Agreement (SLA) issues to | DIR Operations management will include CPO in SLA issues | 1/31/18 | • Director, Operations, COO, |

[8] **Recommendation** – Suggested actions to 1) correct the condition, and 2) address the cause – "what corrective actions are needed". Recommendation are addressed to the DIR executive leadership charged with governance and with the authority and responsibility to implement the recommendation and cause change.
[9] **Action Plan** – Planned course of action to address the recommendation.
[10] **Estimated Completion Date** – Date on which the action plan will be finished.
[11] **Responsible Management Staff** – Executive, director or manager responsible for the implementation and execution of the action plan.

| Recommendation[8] | Management Response | | |
|---|---|---|---|
| | Action Plan[9] | Estimated Implementation Date[10] | Responsible Management Staff[11] |
| contract management staff and include representation from the Chief Procurement Office (CPO) on a panel of at least three individuals authorized to approve or reject SLA exception requests. | reporting, including monthly compliance assessments. Exception decisions will be reviewed by a three-person panel including representatives of COO and CPO divisions. | | • Director, Enterprise Contract Management (ECM), Chief Procurement Office (CPO) |
| B. Develop a RACI chart with defined areas of responsibility and accountability between CPO Contract Management and COO Operations staff for SLA performance management. | DIR management will develop a RACI chart with defined areas of responsibility and accountability between CPO Contract Management and COO Operations for SLA performance management. | 2/28/18 | • Director, Operations, COO<br>• Director, ECM, CPO |
| C. Develop and implement a shared contract and operations management dashboard to report on the categorization of SLA exceptions accepted. | DIR management will work with CPO to develop requirements for SLA exceptions categorization reporting. | 4/1/18 | • Director, Operations, COO<br>• Director, ECM, CPO |
| **Issue 4: Management of SLA Targets** | | | |
| A. Develop a process to standardize legal agreements (bilateral agreements) specific to annual updates to service level performance targets to ensure updates are memorialized in a contract amendment, as required. | DIR management will develop a process and execute a contract amendment that clarifies how service level performance target updates will be formally executed to include authorization by DIR and appropriate vendors. | 9/1/18 | Director, ECM, CPO |
| B. Ensure contract change requests for updates to service level performance targets are documented in the Salesforce System and approved timely by all required parties. | DIR management will ensure contract change requests for updates to service level performance targets are documented and approved timely by all required parties. | 9/1/18 | Director, ECM, CPO |
| **Issue 5: Disaster Recovery Test Plan and Schedule** | | | |
| A. Develop a process to document and retain DIR customers' approval or rejection to schedule Disaster Recovery (DR) tests for eligible "Class 1" and "Class P" applications in IT Service Management Remedy tickets. | DIR will work with the MSI to ensure that customer acceptance or deferral of DCS offered disaster recovery exercises for Class P and Class 1 applications, as documented in the CMDB, are | 7/14/18 | Director, Operations, COO |

| Recommendation[8] | Management Response | | |
|---|---|---|---|
| | Action Plan[9] | Estimated Implementation Date[10] | Responsible Management Staff[11] |
| | documented in ITSM/ Remedy tickets. | | |
| B. Report to the IT Leadership Committee (ITLC) annually the "Class 1" and "Class P" applications not tested, by customer. | DIR management will work with the MSI to provide a summary briefing to the ITLC of the results of annual "Class P" and "Class 1" disaster recovery exercise testing. | 5/15/18 | Director, Operations, COO |
| C. Ensure all eligible "Class 1" and "Class P" applications from the CMDB are included in the fiscal year test plan and schedule before approval. If customers or DIR approve an exception for testing, document the decision on the official schedule based on information available at the time the annual schedule is prepared for DIR approval. | DIR Management will work with MSI to confirm all eligible "Class 1" and "Class P" applications identified in the DCS CMDB are included in the fiscal year test plan and schedule DIR Management will work with MSI to update disaster recovery schedule exercise processes to include creation of an ITSM record documenting any customer or service deferral of disaster recovery exercise testing for Class P or Class 1 applications as offered as part of the DCS. | 6/1/18 | Director, Operations, COO |
| **Issue 6: Disaster Recovery Test Report Timeliness** | | | |
| A. Implement a process to allow DIR customers to formally approve the test results included in their final disaster recovery test reports. | DIR management will work with MSI to update disaster recovery exercise process to include customer sign-off of disaster recovery test reports. | 3/29/18 | Director, Operations, COO |
| B. Implement a process for independent validation of the completed date and time for disaster recovery test reports posted in the DCS Collaboration Portal and used for Service Level Agreement (SLA) measures. | DIR management will work with MSI to implement a process for independent validation of the completed date and time for disaster recovery test reports posted in the DCS Collaboration Portal and used for SLA measurement. | 3/29/18 | Director, Operations, COO |
| C. Update the Functional Requirements Document (FRD) to include posting draft and final test reports in the DCS Collaboration | DIR management will work with MSI as part of the SLA compliance assessment process to update the | 3/29/18 | Director, Operations, COO |

| Recommendation[8] | Management Response | | |
|---|---|---|---|
| | Action Plan[9] | Estimated Implementation Date[10] | Responsible Management Staff[11] |
| Portal for SLA performance target purposes. | functional requirement document (FRD) for the disaster recovery report "Document Delivery Timeliness" SLA to include posting draft and final test reports in the DCS Collaboration Portal for SLA performance measurement purposes. | | |
| **Issue 7: Server Backup Failures** | | | |
| A. Ensure backup failures follow the specified Backup Failure Reporting process, as described in the established procedures PRO-801-05. | DIR management will work with MSI and SCP to develop a semi-annual backup failure reporting quality check process whereby a sample of tickets coded as backup failures are evaluated for compliance with PRO-801-05 and a summary report prepared for DCS management. | 9/1/18 | Director, Operations, COO |
| B. Ensure issues related to backup failures are resolved and resolved timely with complete documentation in the incident tickets. | DIR management will work with MSI and SCP to develop a semi-annual backup failure reporting quality check process whereby a sample of tickets coded as backup failures are evaluated for complete resolution information entry and resolution timeliness and a summary report prepared for DCS management. | 9/1/18 | Director, Operations, COO |
| **Issue 8: Mainframe Backup Process and Reporting** | | | |
| A. Ensure the Service Component Provider (SCP) documents the process in place to implement and accomplish the methodology described in the "Successful Backups – Mainframe" SLA Functional Requirements Document (FRD). | DIR management will work with MSI as part of the SLA compliance assessment process to ensure the SCP documents the process in place to implement and accomplish the methodology described in the "Successful Backups – Mainframe" SLA FRD. | 10/31/18 | Director, Operations, COO |

| Recommendation[8] | Management Response | | |
|---|---|---|---|
| | Action Plan[9] | Estimated Implementation Date[10] | Responsible Management Staff[11] |
| B. Approve the mainframe backup process documented by the SCP. | DIR management will work with MSI as part of the SLA compliance assessment process to approve the mainframe backup processes documented by the SCP. | 10/31/18 | Director, Operations, COO |
| C. Ensure the Multi-Sourcing Integrator (MSI) posts the SCP's approved mainframe backup process documentation in the DCS Collaboration Portal. | DIR management will work with MSI as part of the SLA compliance assessment process to ensure the MSI posts the SCP's approved mainframe backup process documentation in the DCS Collaboration Portal. | 10/31/18 | Director, Operations, COO |
| **Issue 9: Change Request (CRQ) Count Reconciliations** | | | |
| A. Require the MSI to reconcile the change request (CRQ) counts from the DCS Collaboration Portal-ServiceFlow to the CRQ counts from the ITSM-Remedy Ticketing System, and to the final published Enterprise Compliance Report. | DIR management will require the MSI to reconcile the CRQ counts from the DCS Collaboration Portal-ServiceFlow to the CRQ counts from the ITSM-Remedy Ticketing System, and to the final published Enterprise Compliance Report results for the "Change Management Effectiveness" SLA as a point in time check as part of the monthly enterprise SLA compliance validation process. | 4/1/18 | Director, Operations, COO |
| B. Retain documentation of (a) reconciliations performed in the DCS Collaboration Portal and (b) the reconciliation process in the Service Management Manual (SMM). | DIR management will require that MSI retain documentation of reconciliations performed to confirm "Change Management Effectiveness" SLA and document the reconciliation process in the SMM. | 4/1/18 | Director, Operations, COO |
| **Issue 10: CMDB Reconciliation SLAs** | | | |
| A. Establish new Service Level Agreement (SLA) for CMDB accuracy and data quality for all service towers as part of the next Multi-Sourcing Integrator (MSI) contract. | DIR management will establish a new SLA for CMDB accuracy and data quality for all service towers as part of the next MSI contract. The next MSI contract is in negotiations as of 1/9/2018 | 3/1/18 | Director, Operations, COO |

| Recommendation[8] | Management Response | | |
|---|---|---|---|
| | Action Plan[9] | Estimated Implementation Date[10] | Responsible Management Staff[11] |
| | and has not been finalized. DIR expects to have the new MSI Contract in place no later than 3/1/2018. | | |
| B. Continue to involve customers in identifying assets that should be included in the CMDB and in documenting resolution of discrepancies noted, based on the results of reconciliations performed. | DIR management will continue to involve customers in identifying assets that should be included in the CMDB. DIR management will require MSI to present an update on CMDB and customer involvement at one of the "DCS Radio Shows" used as a forum for updating and informing customers about DCS activities. | 7/1/18 | Director, Operations, COO |
| **Issue 11: Backup SLA Data Integrity** | | | |
| A. Require the Service Component Provider (SCP) to develop and document procedures for collecting the source data used for Service Level Agreement (SLA) performance reporting on successful backups. | DIR management will require the SCP to develop and document procedures for collecting the source data used for SLA performance reporting on successful backups. | 7/1/18 | Director, Operations, COO |
| B. Approve the SCP's documented data collection process for SLA performance reporting. | DIR management will approve the SCP's documented data collection process for SLA performance reporting, if appropriate. | 7/1/18 | Director, Operations, COO |
| C. Ensure the Multi-Sourcing Integrator (MSI) posts the SCP's approved data collection process documentation in the DCS Collaboration Portal. | DIR management will ensure the MSI posts the SCP's approved data collection process documentation in the DCS Collaboration Portal. | 7/1/18 | Director, Operations, COO |
| **Issue 12: Update Backup Functional Requirements Document** | | | |
| A. Update the Functional Requirements Document (FRD) for Backup and Recovery to accurately describe where the timeframes for DIR customer backup executions should be maintained. | DIR management will work with MSI as part of the SLA compliance assessment process to update the FRD for Backup and Recovery to accurately describe where the timeframes for DIR customer backup executions, schedules | 2/28/18 | Director, Operations, COO |

| Recommendation[8] | Management Response | | |
|---|---|---|---|
| | Action Plan[9] | Estimated Implementation Date[10] | Responsible Management Staff[11] |
| | retentions, and targets documentation, is maintained. | | |
| **Issue 13: Work Order Status for Successful Recoveries** | | | |
| A. Require the Multi-Sourcing Integrator (MSI) to update the successful recovery procedures to ensure work order statuses accurately represent the results of data restorations and revise the Service Level Agreement (SLA) methodology accordingly. | DIR management will require the MSI and pertinent service providers to update the data recovery procedures to ensure work order statuses accurately represent the results of data restorations and revise the "Successful Recoveries" (Server and Mainframe) SLA reporting methodology so that work order activities that do not result in successful recoveries are reported as service misses subject to SLA exception review for circumstances beyond a service provider's control. | 3/15/18 | Director, Operations, COO |
| B. Revise the SLA reporting methodology to allow for the work orders closed with a status of "Successful with Issues" to include an additional level of detail that summarizes the types and/or cause of issues encountered when attempting to restore DIR customer data. | DIR management will review reporting and processes to ensure that recovery work order field status fields include details to represent the status of data restorations beyond indicating work activities success or not, for example: (a) customer cancelled request, (b) could not find target location, or (c) data was no longer available, etc. | 3/15/18 | Director, Operations, COO |

# Appendix E: Report Distribution

## Internal Report Distribution

Department of Information Resources (DIR) Board

DIR Executive Director

DIR Deputy Executive Director/ State of Texas Chief Information Officer/ State of Texas Cybersecurity Coordinator

DIR Chief Procurement Officer (CPO)

DIR Chief Operations Officer (COO)

DIR COO Operations Director

DIR COO Planning and Governance Director

DIR CPO Enterprise Contract Management Director

## External Report Distribution

Texas Office of the Governor

Texas Legislative Budget Board

Texas State Auditor's Office

Texas Sunset Advisory Commission