

DIR Governance Assessment

Internal Audit Report #16-101

August 2016



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-Hogan, CIA, CISA, CRISC, Director of Internal Audit

Cathy Sherwood, MPA, CPA, CISA, Senior Internal Auditor

Weaver Internal Audit Staff

Alyssa Martin, CPA, Internal Audit Partner

Brian Thomas, CISA, IT Partner

Dan Graves, CPA, Internal Audit Senior Manager

Adam Jones, Strategic Governance Consultant

Marci Sundbeck, CIA, CISA, CFE, Internal Audit Project Manager

Claire Wang, IT Manager

Tareen Alam, Associate

Priyanka Agrawal, IT Associate

Table of Contents

Executive Summary	1
Background.....	4
Detailed Results	6
Objective 1: DIR Governance	9
Issue 1: Charters and Bylaws	10
Issue 2: Board Policies.....	11
Issue 3: Subcommittee Minutes	12
Issue 4: Performance Metrics	13
Issue 5: Staff Development Plans	14
Issue 6: Reporting Guidelines	16
Issue 7: ELT Meeting Structure and Action Items Communication.....	17
Issue 8: Real-time Reporting.....	17
Issue 9: Agency-wide Risk Management	18
Issue 10: Risk Management Plan	19
Objective 2: DIR IT Governance	20
Issue 11: IT Roles, Alignment, and Strategic Plan.....	22
Issue 12: IT Succession Planning	22
Issue 13: IT Strategic Plan	23
Issue 14: IT Goal Prioritization Documentation.....	24
Issue 15: IT Change Management Approval Guidelines.....	24
Issue 16: IT Performance Metrics	25
Issue 17: IT Project Prioritization	26
Issue 18: IT Resource Planning	26
Issue 19: IT Post-Implementation Evaluation.....	27

DIR Governance Assessment

Issue 20: IT Performance Evaluations	28
Issue 21: IT Data Governance	29
Issue 22: IT Process Automation	30
Issue 23: IT Policies and Procedures.....	30
Issue 24: IT Risk Management	31
Appendix A – Objectives, Scope, and Methodologies	32
Objective 1, Scope, and Methodology	33
Objective 2, Scope, and Methodology	35
Appendix B – Maturity Models	37
DIR Governance Maturity Model.....	37
DIR IT Governance Maturity Model.....	39
Appendix C – Management Responses	42
Action Plans	42
Estimated Implementation Dates	42
Responsible Management Staff	42
Appendix D – Report Distribution.....	52
Internal Report Distribution	52
External Report Distribution	52

Executive Summary

This report summarizes the scope, results, and recommendations from the work performed in conducting the Department of Information Resources (DIR) Governance Assessment. This assessment project was included in the Fiscal Year 2016 Internal Audit Annual Plan. The objectives of the assessment were to:

- Assess the design and operating effectiveness of DIR's governance processes, and
- Assess whether the DIR Information Technology governance supports the Agency's strategic goals and objectives, IT resource and performance management are effective, and the risks that may adversely affect the IT function.

As part of the Agency's emphasis on governance, Internal Audit performed procedures to determine the maturity of the DIR's overall governance and governance specific to the Information Technology (IT) function. The scope of the audit concerned the framework and procedures implemented by the DIR Board and the Executive Leadership Team (ELT) to inform, direct, manage, and monitor the activities of the Agency, including the enterprise programs delivered by DIR in alignment with the Agency's strategic objectives.¹ In addition, the audit team reviewed the IT governance of the Agency, consisting of the leadership, organizational structure, policies and processes that ensure the Agency's IT function supports the organization's strategic objectives. The audit did not include evaluations of the unique governance structures of individual enterprise programs of DIR. In addition, the scope of the project did not include a review of ethics, a critical component of governance because a DIR Ethics Evaluation was conducted and reported separately in Internal Audit Report No. 16-102.

DIR exhibits a commitment to improving governance processes throughout the organization. Over the last two years, the Agency has made a concerted effort in a number of areas to improve organizational governance. The Agency has reviewed and revised policies and procedures, improved internal communications, initiated a review of their employee evaluation process and produced a comprehensive Board Member Guide (updated on July 19, 2016) as a resource for their Board members. The onboarding process for new Board members has been well-received by those members starting new terms in 2016.

The audit resulted in 24 issues where a gap existed between the Agency's current governance practices and the goal state of maturity of the Agency. The goal stage of maturity was defined by the Executive Director, Deputy Executive Director and Chief Information Officer (CIO), and the General Counsel of the Agency.

¹ The audit *did not* include an evaluation of the unique governance attributes of each individual enterprise program.

The maturity goal was established based on several factors, including:

- DIR's age and the evolution of its mission and responsibilities,
- Number of state and local agencies served by DIR,
- Number of Texas citizens served directly and indirectly by DIR and,
- Size and nature of DIR programs provided by the Agency.

The issues included in this report are not deficiencies, but areas identified for improvement needed to achieve the governance maturity goal desired by the Agency.

The audit team conducted extensive documentation review covering Agency policies and procedures, Board communications, minutes, operating plans, statutes and administrative rules, and other relevant documents. The team interviewed DIR Board members (both the appointed members and the three ex-officio members), DIR executive management and key personnel charged with the implementation of policies and procedures both for Agency governance and IT governance.

Concurrent with this discovery process, the team developed and customized Agency governance and IT governance maturity models against which the Agency's maturity was evaluated. The Agency governance model was based upon the guidance and criteria established by the National Association of Corporate Directors (NACD)² and the COSO 2013 Internal Control Framework. The IT governance model was based on the criteria established in COSO 2013 Internal Control Framework, the Global Technology Audit Guide (GTAG) 17 – Auditing IT Governance, and COBIT 5 Information Technology Control Framework.

The two models have five key governance areas that are measured on a five-level scale in accordance with industry and government best practices. The governance and IT maturity models and the underlying standards are in Appendix B.

The audit determined the largest gaps in Agency governance maturity are related to the attributes of "Board Oversight" and "Communication and Reporting." The Agency received generally positive results on the maturity attributes of "Policies and Procedures" and "Structure and Accountability", although some gaps still exists with regard to the establishment and management of performance metrics and Human Resource (HR) policies. The audit team also recommended that DIR conduct an Agency-wide Risk Assessment.

Maturity gaps exist in IT governance for the attributes related to "Organization and Governance Structure", "Executive Leadership and Support", and "Strategic and Operational

² DeLoach, Jim. (2015, September). *How Mature Are Your Risk Management Capabilities?* NACD, Retrieved from <https://www.nacdonline.org/Magazine/Article.cfm?ItemNumber=19643>

Planning.” Goal prioritization and change management are two specific areas in which the Agency could improve its processes. IT would benefit from developing performance metrics and establishing a stronger connection with the strategic objectives of the Agency. Larger maturity gaps exist in the maturity attributes of “Service Delivery and Measurement” and “IT Organization and Risk Management.” Automation, IT policies and procedures, and IT risk management had associated issues. DIR management staff indicated that many of these areas were being addressed concurrent with the period of the audit.

DIR management staff concurred with the results and recommendations reported by Internal Audit and provided action plans to implement the recommendations.

Internal Audit would like to thank the Board members, leadership and staff of DIR for their time and participation. All participants were responsive, forthcoming in their communication and generous with their time.

Detailed results of the audit, including the recommendations and management’s responses are documented in the report that follows.

Background

The DIR Governance Assessment was included in the Fiscal Year 2016 Internal Audit Annual Plan. The objectives of the assessment were to:

- Assess the design and operating effectiveness of DIR's governance processes, and
- Assess whether the DIR Information Technology (IT) governance supports the Agency's strategic goals and objectives, IT resource and performance management are effective, and the risks that may adversely affect the IT function.

As part of the Agency's emphasis on governance, Internal Audit performed procedures to determine the maturity of the DIR's overall governance and governance specific to the Information Technology (IT) function. The scope of the audit concerned the framework and procedures implemented by the DIR Board and the Executive Leadership Team (ELT) to inform, direct, manage, and monitor the activities of the Agency, including the enterprise programs delivered by DIR in alignment with the Agency's strategic objectives.³ In addition, the audit team reviewed the IT governance of the Agency, consisting of the leadership, organizational structure, policies and processes that ensure the Agency's IT function supports the organization's strategic objectives. The audit did not include evaluations of the unique governance structures of individual enterprise programs of DIR. In addition, the scope of the project did not include a review of ethics, a critical component of governance because a DIR Ethics Evaluation was conducted and reported separately in Internal Audit Report No. 16-102.

Governance and IT governance were evaluated against separate maturity models developed within professional frameworks from authoritative guidance and national governance associations.

Governance is defined as the combination of processes and structures implemented by the Board or Executive Management to inform, direct, manage and monitor the activities of the organization toward the achievement of its strategic objectives.

Information Technology (IT) Governance is a subset of Agency governance and consists of leadership, organizational structure, and other processes to ensure the IT function supports the Agency's strategic objectives.

DIR provides statewide leadership and oversight for management of government information and communications technology. To manage government information and communications technology, the DIR Board implemented processes and structures to inform, direct, manage, and monitor the activities of the Agency to achieve its strategic objectives. These activities

³ The audit *did not* include an evaluation of the unique governance attributes of each individual enterprise program.

and objectives are executed through multiple enterprise programs that provide services to customer organizations. Enterprise programs operate and deliver services based on their specific and specialized services. Each enterprise program has unique governance attributes that meet the specific needs of the program; however, the specific attributes are executed within the overall Agency governance framework.

Program governance focuses on providing direction and oversight to specific programs to guide the achievement of business outcomes and to provide data and feedback on the desired results for the overall business strategy. Program governance is executed by DIR Executive Management to provide oversight, structure, and policies that define management principles and decision making. Program governance includes:

- **Organizational Structures:** program steering committees, a program management office, and an organizational model;
- **Roles:** executive sponsor(s), steering committee member(s), program director/manager, and project managers; and
- **Mechanisms:** program policies, decisions or authoritative specifications for program guidance and direction.

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 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.

Detailed Results

In summary, gaps exist between the governance maturity goals, as determined by DIR executive management, and the current maturity states of Agency governance and IT governance. DIR has implemented many processes and procedures in place. However, DIR needs formalize and define these processes and procedures to operate at the maturity levels desired by executive management.

To evaluate the maturity of DIR's governance and IT governance, Internal Audit interviewed key DIR leadership and Board members, reviewed documentation, and assessed the overall design of DIR's governance and IT governance processes. The current maturity of the Agency was compared to the maturity attributes and characteristics defined in the guidance and criteria established by the National Association of Corporate Directors (NACD), the COSO 2013 Internal Control Framework, the Global Technology Audit Guide (GTAG) 17 – Auditing IT Governance, and COBIT 5 Information Technology Control Framework (Appendix B.)

To evaluate Agency governance, Internal Audit evaluated the maturity of DIR's structure and operating practices against the five attributes of the governance model and the characteristics of those attributes.

For the attribute of **Board Oversight**, the audit team evaluated the Board policies adopted and the charter(s) or bylaws for the Board and its subcommittees. Board policies were evaluated to determine if the content of the policies was appropriate and provided guidance for the governance of the Agency. Internal Audit also evaluated the meeting minutes and materials for the Board and its subcommittees for the period October 1, 2015 through March 31, 2016 to determine the level and detail at which the actions and discussions of the Board and its subcommittees were memorialized.

Strategy, Policies, and Procedures included a review of the current DIR Strategic Plan and a sample of DIR policies and procedures to assess how they supported the Agency's goals, mission, and objectives. Auditors also assessed whether the Agency had appropriately defined performance metrics that 1) align with DIR's Strategic Plan and 2) provide meaningful information to monitor the Agency's performance and accomplishment of the initiatives within the plan.

The **Structure and Accountability** attribute included a review of staff hiring, evaluation, and training processes. In addition, the audit team reviewed the procedures to evaluate the effectiveness of hiring, training, staff development, and communicating roles and responsibilities. Internal Audit reviewed a sample of job descriptions, performance evaluations, and training records to determine the detail of which responsibilities were communicated, the monitoring and communication of employee performance, and the efforts of the Agency to manage and monitor staff development. The succession planning for the

Executive Leadership Team (ELT) was also evaluated to determine whether the Agency had appropriately planned for staff continuity.

Communication and Reporting included policies, procedures, and activities to assess the methods in which DIR disseminated information to stakeholders both internally and externally to the Agency. Auditors reviewed the communications used by DIR Board and staff, including Board meeting minutes, ELT meeting notes, status reports, formal and informal reports, public information on the DIR website, and a sample of communications provided to customers to determine whether the Agency effectively communicated information. The availability of real-time reporting as well as the monitoring and reporting of performance metrics and the achievement of DIR's goals and strategic objectives were also evaluated to determine if communication and reporting provided information to the Board, management, and staff of DIR.

Risk Assessment included the processes in place to support how DIR met its stated objectives including risk assessment and management processes, monitoring plans, and compliance plans. Auditors evaluated the processes in place to identify, assess, and manage risks inherent to the Agency as a whole. The Agency's processes to develop a risk management plan and to perform ongoing risk monitoring were included in the evaluation of the risk assessment processes.

To evaluate IT governance, Internal Audit assessed the IT **Organization and Governance Structure** that included internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence the governance design. Auditors evaluated the formal and informal governance bodies in place, including the ELT and the Change Management Board, and evaluated the production deployment processes for sufficiency and effectiveness. The strategic plan was inspected to determine whether organization needs and IT service requirements were clearly defined in the plan. Auditors also reviewed job descriptions for IT management.

The **Executive Leadership and Support** attribute for the IT function included the inspection of the DIR's internal website, the Strategic Plan, and Agency and division goals to determine whether the roles and responsibilities of the IT function were clearly defined and communicated. Internal Audit reviewed a sample of project status reports that were provided to the ELT for discussion and prioritization of IT service delivery projects related to the Agency's strategic and tactical plans. Auditors also inspected the IT budget for Fiscal Year 2016 to evaluate the processes performed by management to ensure that IT had adequate planning and funding to meet the Agency's needs.

The evaluation of the **Strategic and Operational Planning** attribute included an inspection of the IT roadmap to determine whether it took into account IT requirements, deliverables, and supported the Strategic Plan. Internal Audit evaluated the procedures DIR's IT function used to articulate its value and the key performance metrics used by DIR ELT to measure and monitor the effectiveness of the IT function. Auditors inspected the performance

evaluations for IT management to determine whether the performance evaluations evaluated individual performance against the overall division goals and responsibilities. Internal Audit also reviewed a sample of ongoing IT projects to determine the procedures performed to select, prioritize, and evaluate IT projects. The procedures were evaluated to determine if a cost-benefit analysis was performed for each project and whether a plan was developed that included the determination of the resource capacity and manpower required to complete the project. A sample of completed IT projects was reviewed to determine whether the results and quality were evaluated after implementation against the pre-defined targets, and whether lessons learned were factored into future IT investment decisions. Auditors evaluated the planning process used by IT to determine whether their Resource Plan considered the current and future need for IT-related resources, options for resourcing (including sourcing strategies), allocation of resources, and management principals to meet the needs of the enterprise in an optimal manner.

Service Delivery and Management included the inspection of documentation to determine how IT costs were tracked against budget, and determined the frequency in which IT costs were reported to the Board and ELT. Auditors selected a sample of reports to validate that the reports were provided to the Board and ELT on a quarterly basis. Internal Audit also evaluated the contract management and monitoring process and practices to determine whether IT-related contracts were tracked and monitored.

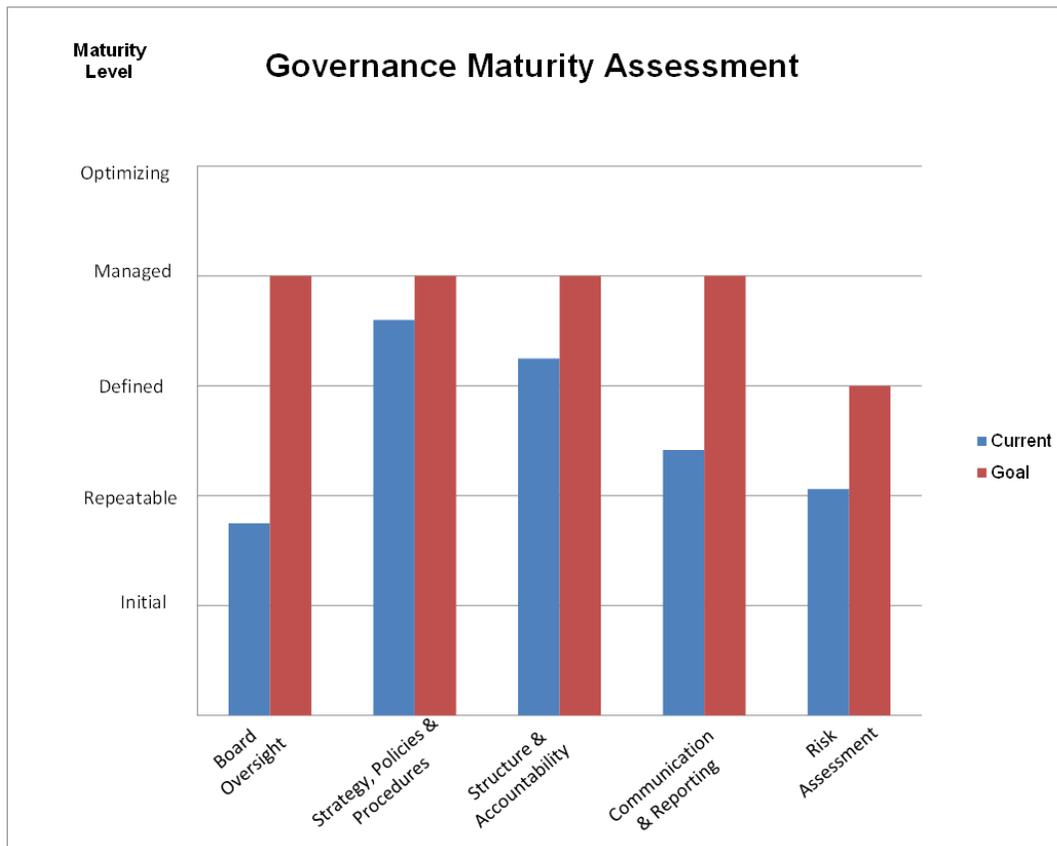
The **IT Organization and Risk Management** attribute was inspected through the evaluation of data management policies and procedures and the degree of automation within IT's organizational processes. Auditors reviewed the data automation assessment performed by IT. Internal Audit evaluated the IT function's policies and procedures, including the IT security framework and standards, to ensure they were complete, reviewed, approved, and updated on a regular basis. Auditors also inspected IT Risk Assessment documentation to evaluate whether the risk profile and risk appetite thresholds were monitored by DIR management, and whether the risk management strategy aligned with the enterprise risk strategy.

The following maturity achievement charts represent the goal maturity levels of the Agency's governance and IT governance processes and Internal Audit's assessment of the current state of maturity. A summary chart is presented for each objective, governance and IT governance, respectively. Additional charts display the separately assessed and goal maturity levels for each of the five attributes for governance and the five attributes for IT governance. The issues in each attribute area identify where the current state of DIR's maturity is not aligned to the desired maturity level (maturity goal) of the Agency in relation to the elements for each attribute. Where an issue affects more than one governance attribute, Internal Audit referenced the issue in all the attributes affected by the condition.

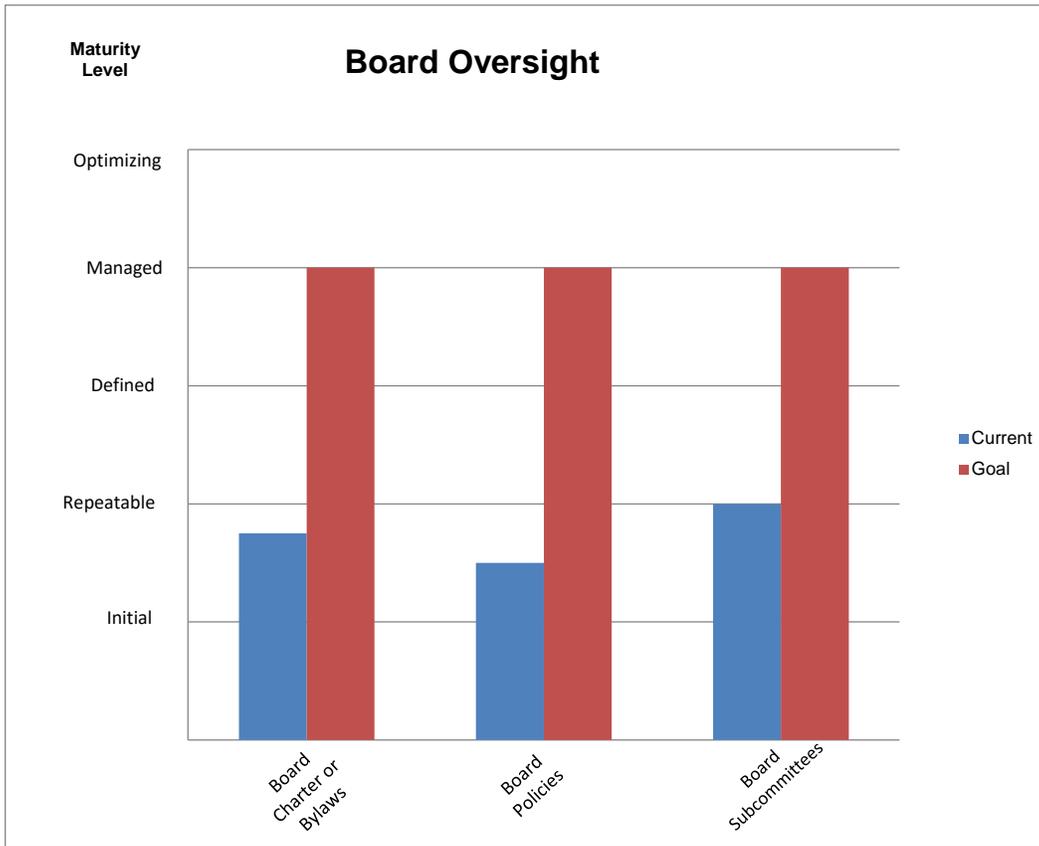
DIR Governance

We assessed the design and operating effectiveness of DIR’s governance processes. We evaluated the governance structure in its current condition against a governance maturity model to determine the level of maturity of the Agency’s governance processes. See Appendix B for the maturity model against which the Agency was evaluated.

Overall DIR Governance Conclusion



Board Rules and Oversight



Issue 1: Charters and Bylaws

Only one of the seven Board subcommittees, the Finance and Audit Subcommittee, has a written charter or bylaws. The other six subcommittees do not have a charter or bylaws to define the roles, authorities, responsibilities, structures, meeting frequency, and documentation and approval of meeting minutes of the Board and its subcommittees. The following Board subcommittees do not have charters:

- Communication Technology Services (TEX-AN/CCTS) and Information Security
- Data Center Services (DCS)
- Historically Underutilized Businesses (HUBs) and Cooperative Contracts
- Texas.gov
- Personnel
- Strategic Oversight

Recommendations:

To mature the DIR Governance to a “Defined” or “Managed” state, DIR management should:

Defined: Establish formal charters or bylaws for the Board subcommittees to outline the responsibilities and reporting requirements for each body. Charters should include the following:

- Subcommittee's charge or mission statement
- Authority and responsibilities of the Subcommittee
- Composition of the Subcommittee
- Meeting frequency
- Documentation and approval of meeting minutes

Managed: Conduct recurring meetings with documented and approved meeting minutes for a sustained time period of six to 12 months.

Management Response:

DIR management agreed with Internal Audit’s recommendations.

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

Issue 2: Board Policies

The current Board policies provide limited detail, guidance and direction on executing and fulfilling the statutory requirements of Texas Government Code (TGC) Chapter 2054. Four of the eight existing DIR Board policies are restatements of the TGC 2054:

- TGC, Chapter 2054.041 (a) / Texas Administrative Code (TAC) 201.4 (d)
- TGC, Chapter 2054.041 (b) / TAC 201.4 (e)
- TGC, Chapter 2054.041 (c) / TAC 201.4 (f)
- TGC, Chapter 2054.040 / TAC 201.4 (g)

Recommendations:

To mature the DIR Governance to a “Defined” or “Managed” state, DIR management should:

Defined: Update Board policies to provide detailed guidance and direction on how Agency management will fulfill the statutory requirements of the TGC and the Agency’s strategic goals.

Managed: Conduct reviews and updates of policies on a regular basis to ensure the policies are up-to-date and relevant for the Agency. Reviews should occur at least annually.

Management Response:

DIR management agreed with Internal Audit's recommendations.

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

Issue 3: Subcommittee Minutes

Meeting minutes are not prepared, approved and maintained for the subcommittees of the Board. Notes are maintained by meeting attendees. However, those notes are not approved to memorialize the discussions and staff actions requested by the subcommittees.

Recommendations:

To mature the DIR Governance to a "Defined" or "Managed" state, DIR management should:

Defined: Prepare and review minutes of each Subcommittee that are approved by the Subcommittee. These minutes should be retained in a central repository with appropriate access restrictions to the Board and members of the Executive Leadership Team.

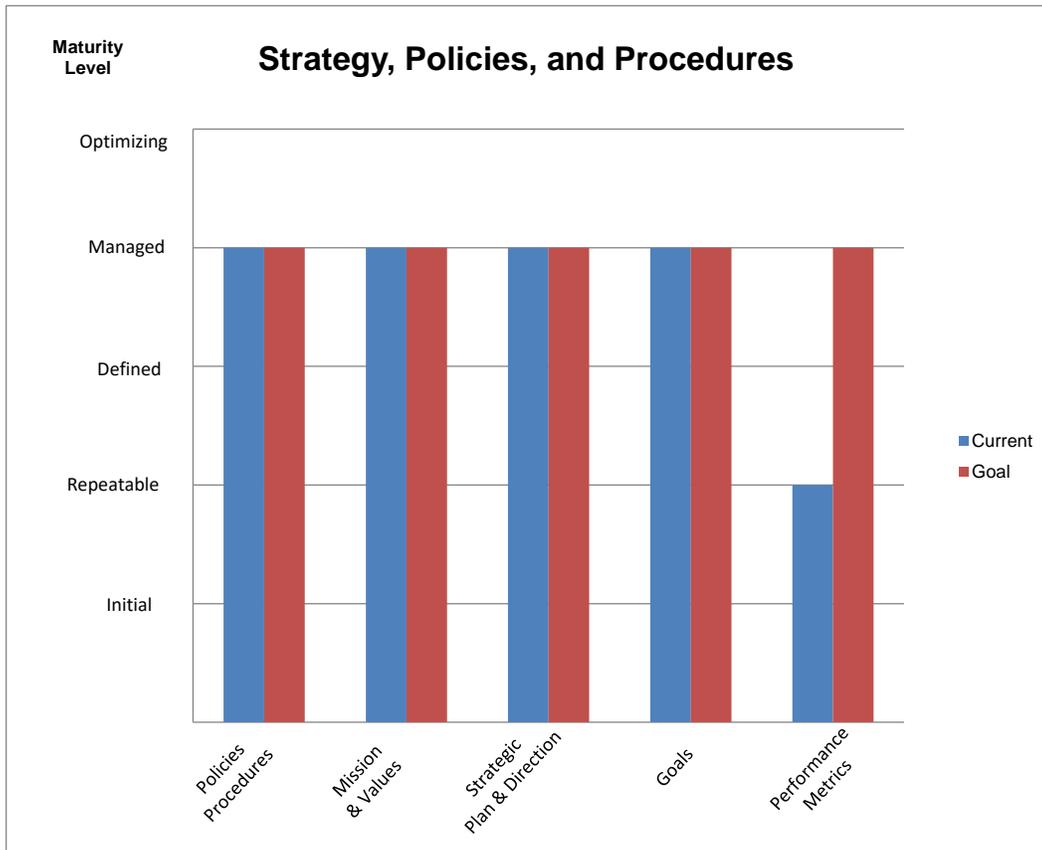
Managed: Conduct recurring meetings with documented and approved meeting minutes for a sustained time period of six to 12 months.

Management Response:

DIR management agreed with Internal Audit's recommendations.

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

Strategy, Policies, and Procedures



Issue 4: Performance Metrics

Agency-wide performance metrics that align with DIR’s Strategic Plan are not formally defined, monitored, and reported. DIR monitors and reports the performance measures required by the Legislative Budget Board (LBB). However, meaningful performance metrics to measure the achievement of the goals and objectives of the Strategic Plan are not defined.

Recommendations:

To mature the DIR Governance to a “Defined” or “Managed” state, DIR management should:

Defined: Identify metrics that provide meaningful information to monitor the Agency’s performance and accomplishment of the key strategic initiatives from the approved strategic plan.

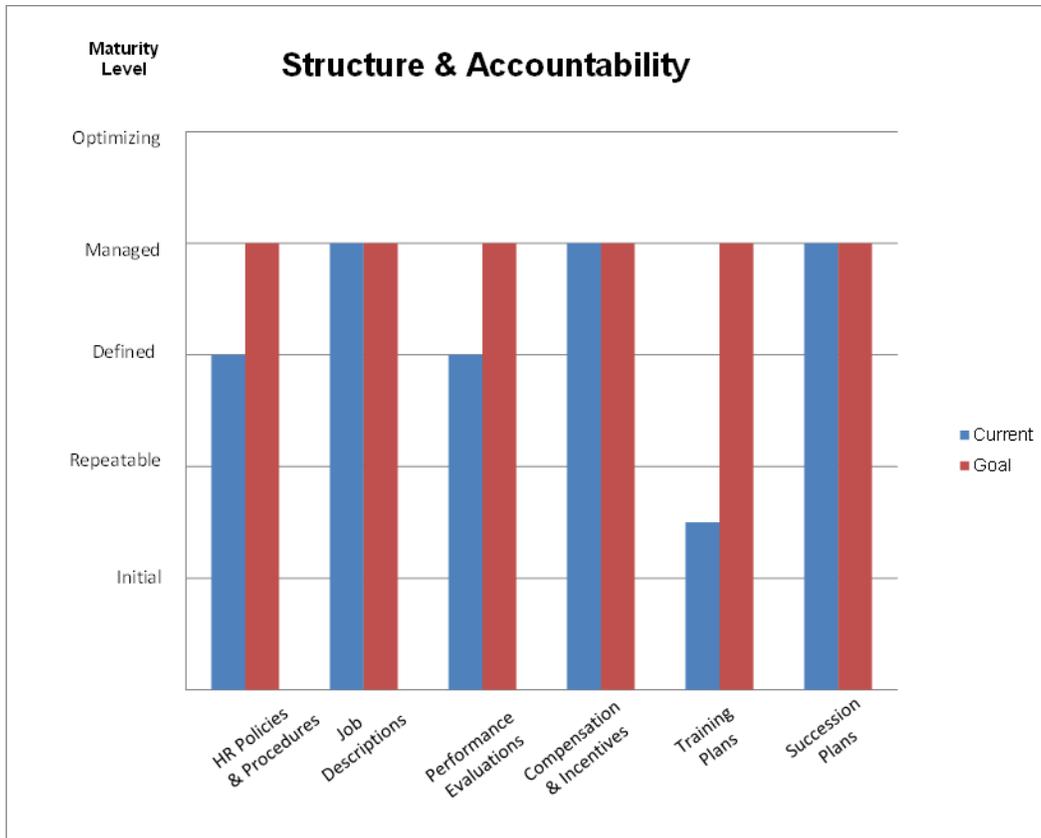
Managed: Define processes to monitor and consistently report the metrics to DIR Management and the Board. Dashboards should be developed to accurately report the outcome of the performance metrics to all applicable users.

Management Response:

DIR management agreed with Internal Audit’s recommendations.

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

Structure and Accountability



Issue 5: Staff Development Plans

Continuing professional education and training plans to manage and monitor staff development of Agency personnel have not been established to maintain or enhance the competencies needed by staff to properly execute their job responsibilities. Professional development training is available to employees upon request, but there are no requirements to identify and complete relevant continuing education. However, DIR Human Resources does track required trainings for:

- Ethics
- Security

- Electronic and Information Resources (EIR) Accessibility
- Diversity, Equal Opportunity and Non-Discrimination
- Safety

Recommendations:

To mature the DIR Governance to a “Repeatable”, “Defined” or “Managed” state, DIR management should:

Repeatable: Establish a development and training plan for each employee level within DIR. The development and training plan should include continuing education for professional certification requirements and professional development training to maintain and improve the skill sets and knowledge of staff that is required to perform their job duties.

Defined: Document the expectations for the training plans for each level of employee that include the expected number of hours of training, training budgets and expected timeframes of completion.

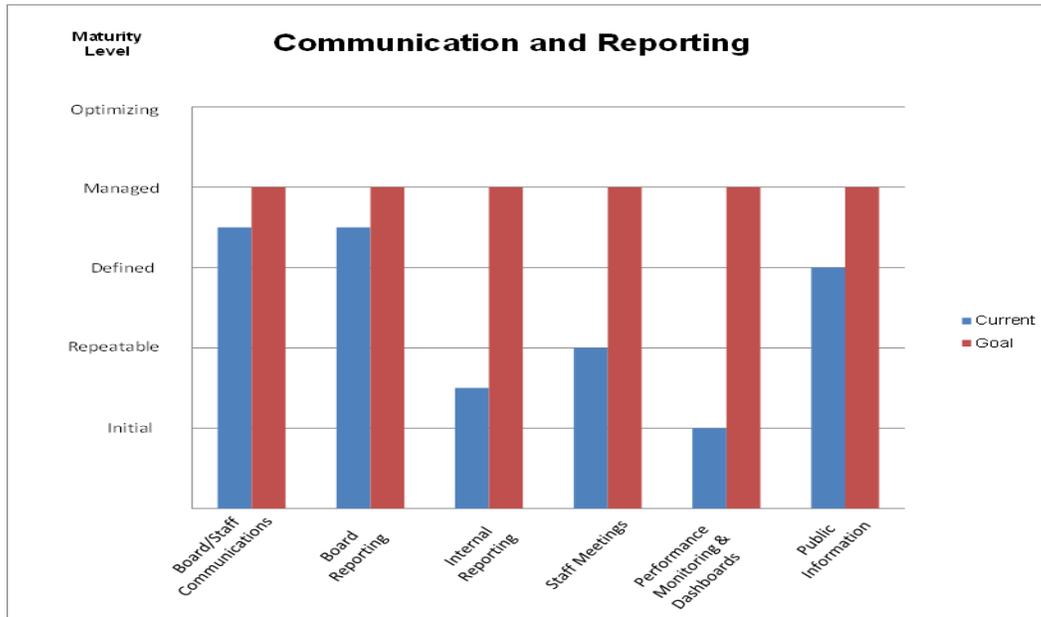
Managed: Monitor the completion of the training plans to ensure that employees have current and relevant knowledge and skills for their function within the Agency.

Management Response:

DIR management agreed with Internal Audit’s recommendations.

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

Communication and Reporting



Issue 6: Reporting Guidelines

There are no Agency-wide, approved communication guidelines that provide instruction to Agency personnel or establishes standards and requirements for Agency communications. Guidelines should address the appropriateness of content for specific audiences and the approval of communications prior to their release.

Recommendations:

To mature the DIR Governance to a “Defined” or “Managed” state, DIR management should:

Defined: Establish and document formal guidelines and standards for Agency communications involving appropriate content for audiences and procedures to obtain approval before the release of communications to the intended user.

Managed: Implement controls to approve and monitor communication releases to ensure communications are in accordance with established guidelines.

Management Response:

DIR management agreed with Internal Audit’s recommendations.

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

Issue 7: ELT Meeting Structure and Action Items Communication

The regular meetings of DIR's Executive Leadership Team (ELT) are not guided by a standing agenda to outline the routine discussion items of the ELT. Documented communication of the commitments, prioritization of projects, or determinations made in the ELT meetings are not produced to disseminate the information to the ELT or provide a tool in which accountability can be established for action items.

Recommendations:

To mature the DIR Governance to a "Defined" or "Managed" state, DIR management should:

Defined: Incorporate a standing agenda into the reoccurring calendar invitation to the ELT members to provide a guideline for the direction and content and of the ELT meetings. The standing agenda would document the recurring discussion items based on their respective frequency.

Managed: Prioritize decisions made on IT projects by the ELT and document any action items to communicate commitments and establish accountability. This documentation could occur via an email from the Executive Director, or their Administrative Assistant, to the ELT summarizing the action items or decisions made.

Management Response:

DIR management agreed with Internal Audit's recommendations.

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

Issue 8: Real-time Reporting

The Agency does not have dashboards or other formats of real-time or near real-time monitoring and communication of performance metrics and performance management. Communication and monitoring of Agency performance is performed periodically, or on an ad hoc basis. Due to the Agency has limited performance metrics to manage the operations of DIR, real-time monitoring and reporting are not in place.

Recommendations:

To mature the DIR Governance to a "Defined" or "Managed" state, DIR management should:

Defined: Design real-time or near real-time methods to monitor and report performance to the ELT and the Board, once performance metrics have been identified and established.

Managed: Develop reporting methods that actively disseminate information to be used to make operational and management decisions. This could be accomplished by dashboards

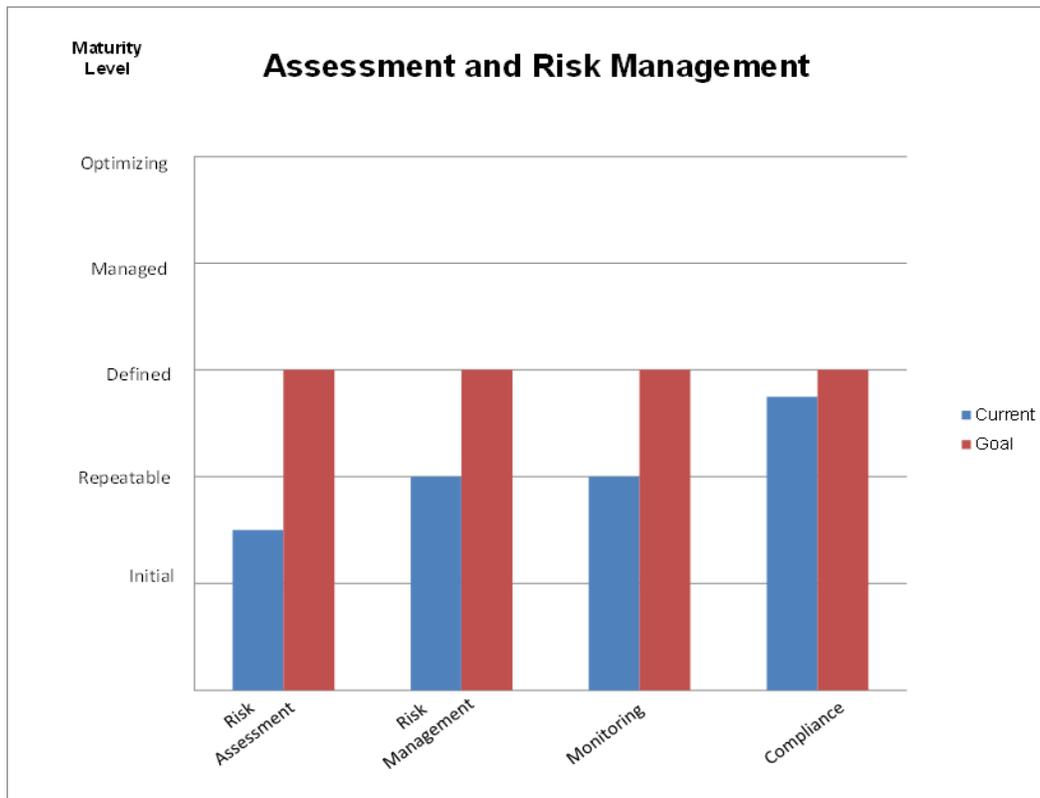
that display upon login to DIR systems, daily flash reports, or systematic notifications to personnel responsible for monitoring and executing activities that affect the metrics.

Management Response:

DIR management agreed with Internal Audit’s recommendations.

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

Assessment and Risk Management



Issue 9: Agency-wide Risk Assessment

DIR has not performed an Agency-wide Risk Assessment to identify, assess, manage, and control events and situations relevant to the operations of DIR. The Agency has performed an Internal Audit Risk Assessment that is utilized for the development of the annual Internal Audit Plan. The Internal Audit Risk Assessment and Internal Audit Plan are elements of the response to risks to the Agency, but do not constitute an Agency-wide Risk Assessment.

Recommendations:

To mature the DIR Governance to a “Repeatable” or “Defined” state, DIR management should:

Repeatable: Develop an Agency-wide Risk Assessment to assist DIR in identifying and mitigating the risks to accomplishing the mission and objectives. The Risk Assessment should consider risks that negatively affect the accomplishment of objectives and that is related to, but not limited to, operations, strategy, legislation, compliance, and financial processes.

Defined: Determine and establish a recurring process to periodically update the Risk Assessment to ensure the assessment reflects the current risk profile of the Agency.

Management Response:

DIR management agreed with Internal Audit's recommendations.

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

Issue 10: Risk Management Plan

The Agency does not have a documented Risk Management Plan in place to manage and monitor the risks that influence DIR and its operations. The ELT appears to be aware and cognizant of the risks that face the Agency, but no documented Risk Management Plan and strategy exists for the Agency.

Recommendation:

To mature the DIR Governance to a "Defined" state, DIR management should:

Defined: Develop an Agency Risk Management Plan to mitigate risk to an acceptable level for Management and the Board, as well as monitor the risks to ensure that they do not exceed the tolerable thresholds, once DIR has implemented the Agency-wide Risk Assessment.

Management Response:

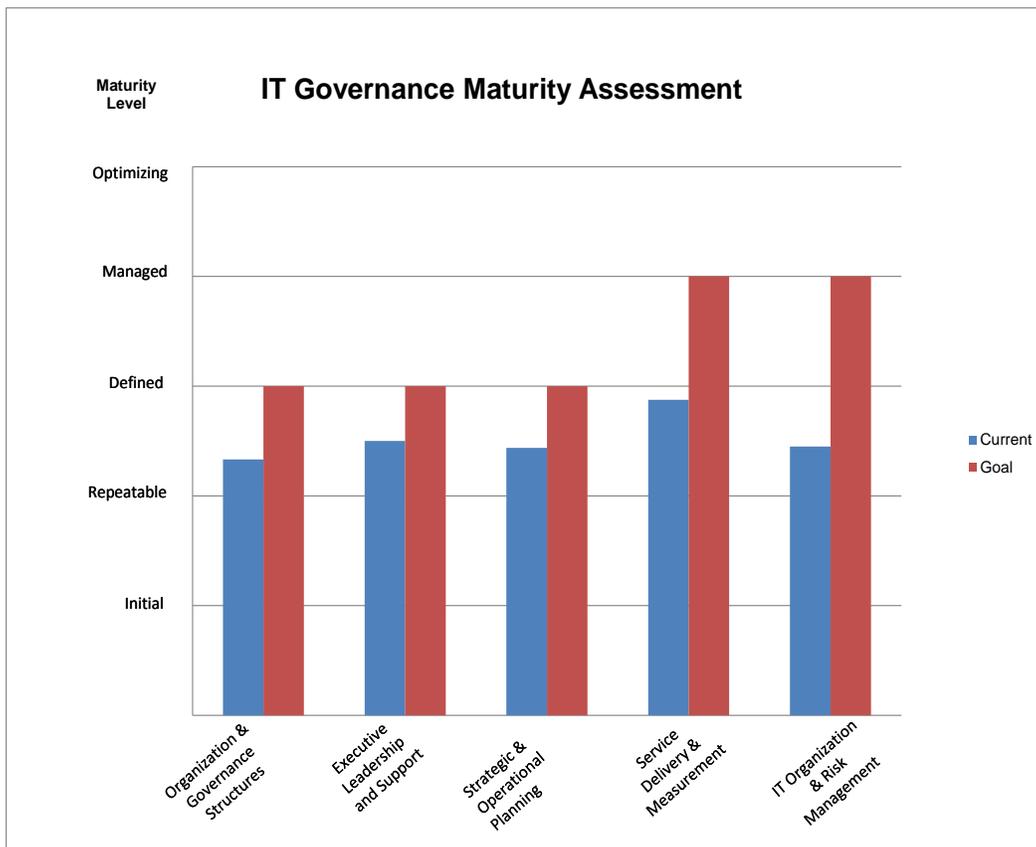
DIR management agreed with Internal Audit's recommendations.

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

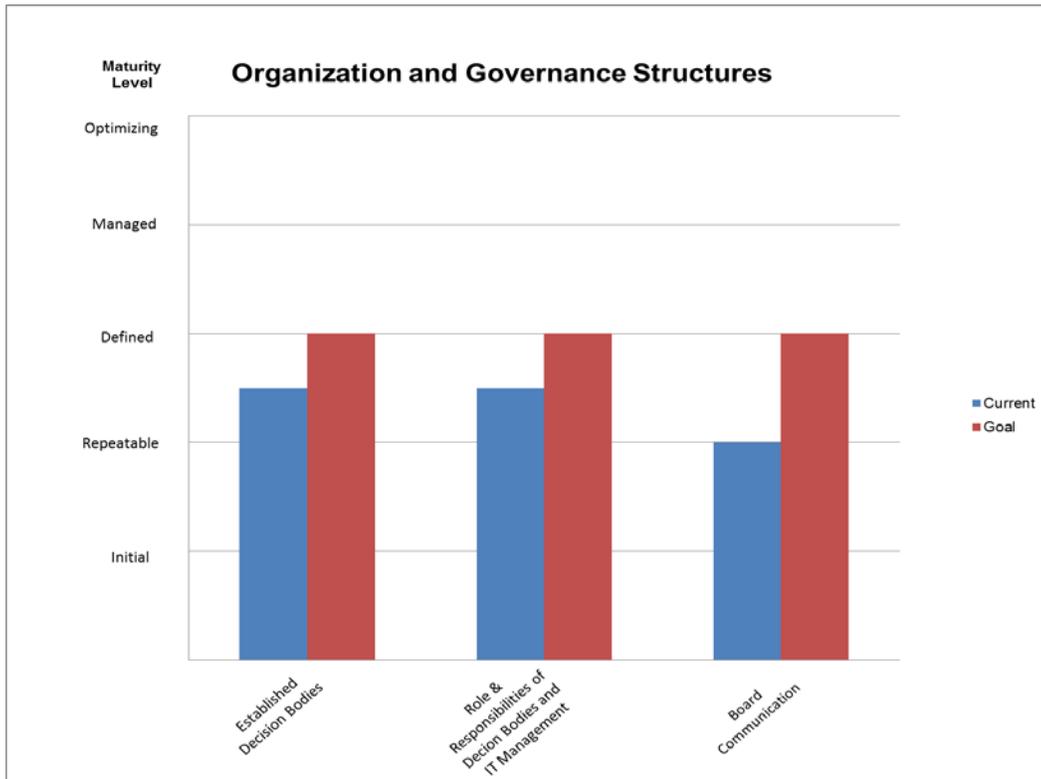
DIR IT Governance

We assessed whether the DIR Information Technology governance supports the Agency's strategic goals and objectives, IT resource and performance management are effective, and the risks that may adversely affect the IT function. We evaluated the IT governance structure in its current condition against an IT governance maturity model to determine the level of maturity of the Agency's IT governance processes. See Appendix B for the maturity model against which the Agency is evaluated.

Overall DIR IT Governance Conclusion



Organization and Governance Structures



Issue 1: Charters and Bylaws

This issue is discussed in Objective 1: DIR Governance and also applies to Objective 2: DIR IT Governance.

Issue 3: Subcommittee Minutes

This issue is discussed in Objective 1: DIR Governance and also applies to Objective 2: DIR IT Governance.

Issue 7: ELT Meeting Structure and Action Items Communication

This issue is discussed in Objective 1: DIR Governance and also applies to Objective 2: DIR IT Governance.

Issue 11: IT Roles, Alignment, and Strategic Plan

The Agency's Strategic Plan does not clearly define the role of Information Technology Services (ITS) for supporting the organization's strategic objectives. The roles and responsibilities of ITS and its governance decision bodies are not clearly defined or communicated to ensure that their roles are still well understood throughout the Agency.

Recommendation:

To mature the DIR IT Governance to a "Defined" state, DIR IT management should:

Defined: Document the roles and responsibilities of Agency IT and the IT governance decision bodies and formally communicate them to all DIR employees via the internal forums such as the DIR internal portal.

Management Response:

DIR IT management agreed with Internal Audit's recommendations.

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

Issue 12: IT Succession Planning

The succession plan for Information Technology Services (ITS) personnel does not include details of the timelines, hand-off process, training, assessment and monitoring executed as part of a transition. ITS has a defined successor for the two key leadership positions of the Chief Technology Officer (CTO) and the Director of ITS also the Information Resources Manager (IRM). However, there is not a documented transition plan for planned changes or clearly defined skills and operational knowledge required of successors to aid in the transition in the event that a leader is suddenly unavailable.

Recommendation:

To mature the DIR IT Governance to a "Defined" state, DIR IT management should:

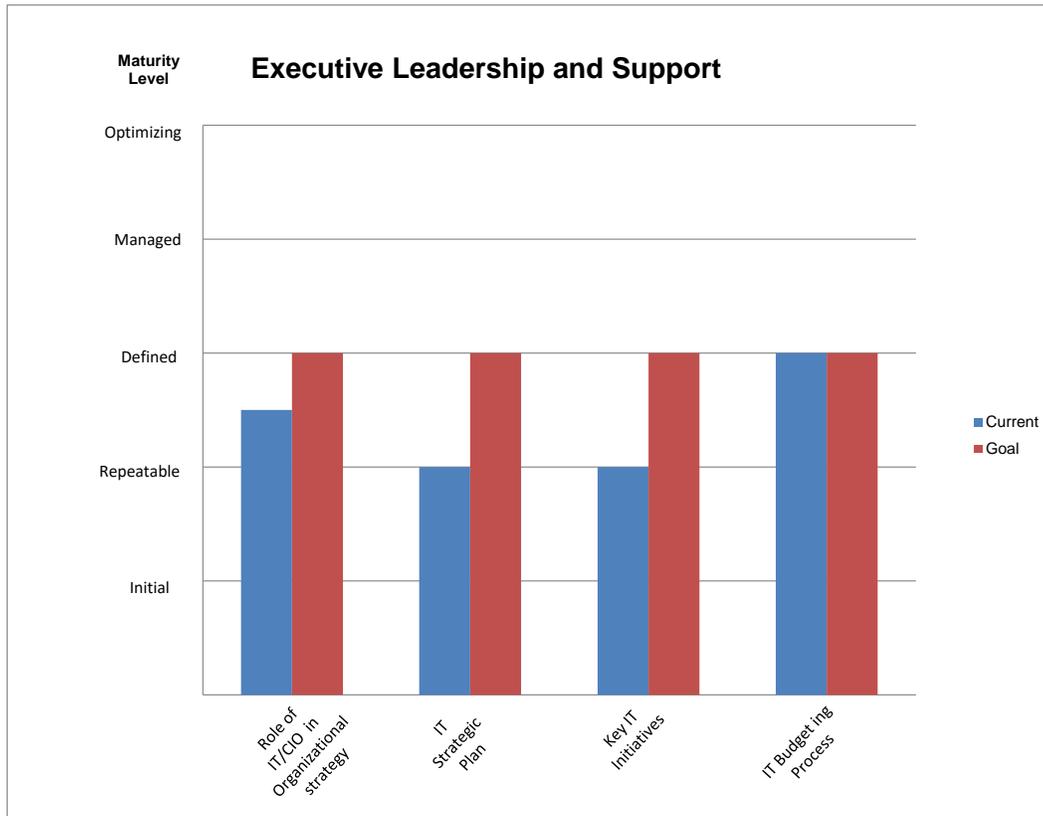
Defined: Document a well-defined Succession Plan for the key leadership positions that includes the name of the successor and that provides guidance, training, information, and the tools needed to support a successful succession.

Management Response:

DIR IT management agreed with Internal Audit's recommendations.

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

Executive Leadership and Support



Issue 13: IT Strategic Plan

An IT-specific Strategic Plan is not documented to demonstrate the Information Technology Services (ITS) alignment with the Agency’s Strategic Plan. The Agency’s Strategic Plan contains high level strategic goals without detailed directions and metrics for the expectations, monitoring, and measurement of the ITS’s performance in achieving their strategic objectives. In addition, the performance goals defined in the Agency’s roadmap are not measured on a periodic basis.

Recommendation:

To mature the DIR IT Governance to a “Defined” state, DIR IT management should:

Defined: Create an IT Strategic Plan that defines the ITS’s strategy for helping DIR fulfill the Agency’s overall Strategic Plan. Alternatively, this could be accomplished as an appendix to the existing Agency Strategic Plan. This should include the mechanism for how ITS is measured in terms of supporting and enabling the achievement of goals defined within the Strategic Plan. It should also establish the foundation for quantifiable performance measures that help demonstrate the true value provided by ITS.

Management Response:

DIR IT management agreed with Internal Audit's recommendations.

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

Issue 14: IT Goal Prioritization Documentation

There is no documentation for establishing the considerations, inputs, and rating results from the ELT's prioritization and assessment of the Agency's top 13 goals to ensure they aligned with DIR's strategic objectives. Agency leadership performed this assessment, but did not retain documented information about the impact and effort of the goals on the DIR's strategic objectives.

Recommendation:

To mature the DIR IT Governance to a "Defined" state, DIR IT management should:

Defined: Define the assessment parameters for determining the Agency's top priority goals and retain documentation on goals selection and assessment results. ELT meetings on the prioritization of goals should be documented for transparency and accountability purposes.

Management Response:

DIR IT management agreed with Internal Audit's recommendations.

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

Issue 15: IT Change Management Approval Guidelines

There are no documented guidelines to specify the types and/or size of projects that require presentation to the Change Control Board (CCB) or discussion and approval during Change Management meetings. Projects are currently presented for discussion and approval on an ad hoc basis. Additionally, there is no formal methodology to estimate the project hours and resources required to complete the changes needed.

Recommendation:

To mature the DIR IT Governance to a "Defined" state, DIR IT management should:

Defined: Establish documented guidance on the type of projects that are required to be discussed in the Change Management meetings. The guidance should include specifications for the types of information to submit to the CCB including details on the size of the projects

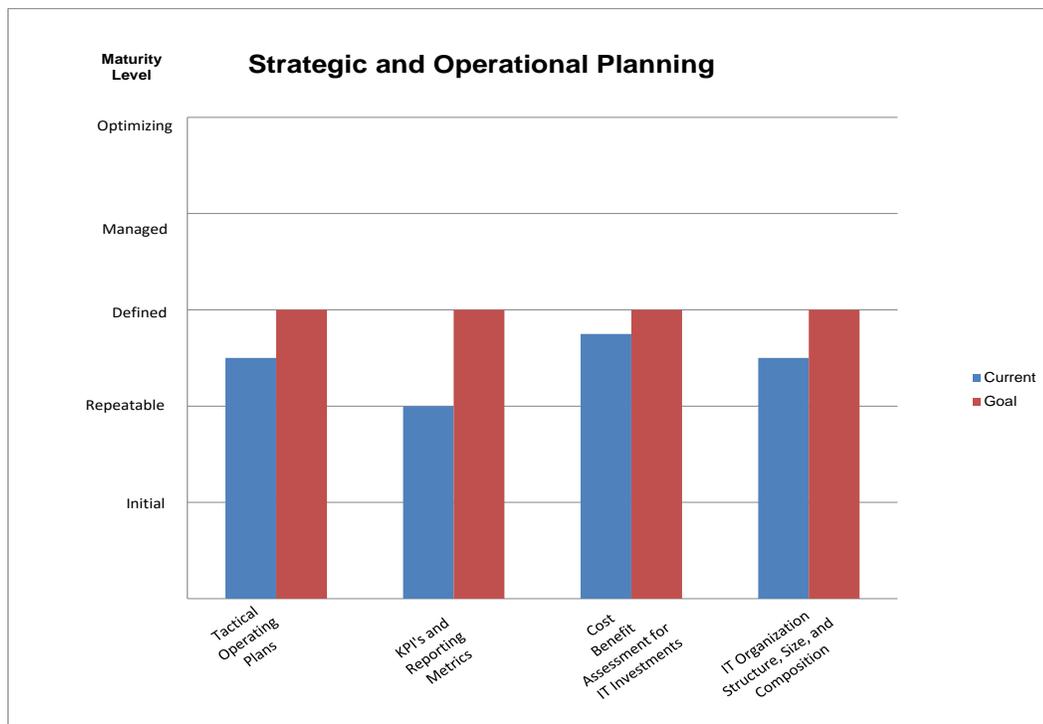
(in terms of hours), cost, the type of project, relationship to strategic and tactical plans, and any other criteria the CCB may consider beneficial for decision making purposes.

Management Response:

DIR IT management agreed with Internal Audit’s recommendations.

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

Strategic and Operational Planning



Issue 16: IT Performance Metrics

The key performance indicators (KPIs) to measure, monitor, and periodically report the overall effectiveness of Information Technology Services (ITS) are not defined. The Agency monitors performance measures required by the Legislative Budget Board (LBB). However, the lack of IT-specific performance metrics limits the ability of ITS to measure and articulate the value that ITS is providing to DIR. The performance goals defined in the Agency’s roadmap are not consistently defined, quantified and measured.

Recommendation:

To mature the DIR IT Governance to a “Defined” state, DIR IT management should:

Defined: Define KPIs that measure the effectiveness of ITS based upon Service Level Agreements (SLAs) and key strategic and tactical plans. The KPIs should be measured on a periodic basis to ensure that ITS’s performance is meeting Agency requirements.

Management Response:

DIR IT management agreed with Internal Audit’s recommendations.

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

Issue 17: IT Project Prioritization

The project prioritization process is informal and does not have established evaluation and classification criteria such as a cost-benefit analysis or Return on Investment (ROI) evaluation. The criteria and methodology used to prioritize projects in the ELT meetings is not documented.

Recommendation:

To mature the DIR IT Governance to a “Defined” state, DIR IT management should:

Defined: Ensure that any action items and prioritization decisions of IT projects made in the ELT meetings are documented to communicate the commitments and establish accountability. A detailed cost-benefit analysis should be performed to quantify the expected project results. The prioritization of projects should be based on this numerical assessment of the cost-benefit analysis/ROI, along with other criteria as deemed appropriate by the ELT.

Management Response:

DIR IT management agreed with Internal Audit’s recommendations.

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

Issue 18: IT Resource Planning

DIR IT does not have a documented process for conducting IT resource planning that demonstrates the current and future need for IT-related resources, options for resourcing (including sourcing strategies), and allocation and management principals to meet the needs of the enterprise in an optimal manner.

Recommendation:

To mature the DIR IT Governance to a “Defined” state, DIR IT management should:

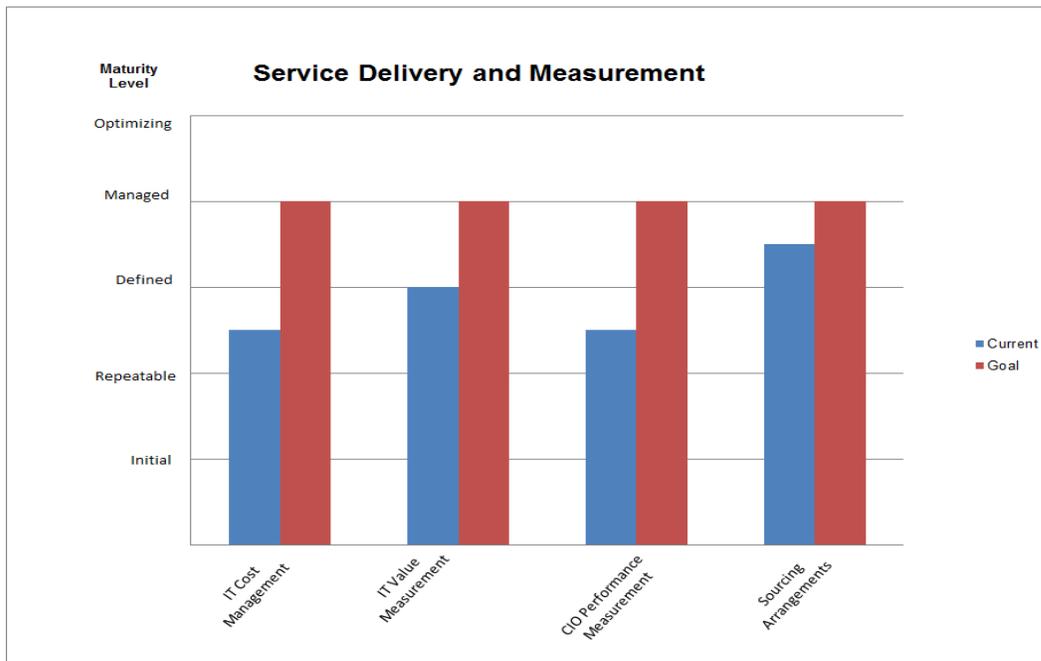
Defined: Document its resource planning process. The process should describe how the current and forecasted future resource requirements are considered and planned, including options for resourcing and sourcing strategies.

Management Response:

DIR IT management agreed with Internal Audit’s recommendations.

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

Service Delivery and Measurement



Issue 19: IT Post-Implementation Evaluation

Project post-implementation reviews are not documented. A documented review should include a comparison of project results against pre-defined success targets and lessons learned to ensure the knowledge gained is carried forward to future IT investment decisions.

Recommendations:

To mature the DIR IT Governance to a “Defined” or “Managed” state, DIR IT management should:

Defined: Pre-define and communicate the targets and criteria against which the success of a project will be evaluated. Targets should include budgetary and cost-benefit goals.

Managed: Ensure that projects are evaluated post implementation to compare their results and quality with pre-defined success targets. Such evaluations should also include analysis of actual budget results against those included in the initial cost-benefit. Lessons learned should be documented and factored into future IT investment decisions.

Management Response:

DIR IT management agreed with Internal Audit's recommendations.

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

Issue 20: IT Performance Evaluations

Performance evaluations for IT Senior Management are currently based on job description only and not aligned to evaluate the performance of the managers towards achieving the overall goals or responsibilities of Information Technology Services (ITS) and the Agency.

Recommendations:

To mature the DIR IT Governance to a "Defined" or "Managed" state, DIR IT management should:

Defined: Pre-define and communicate the criteria to include in the evaluations IT Senior Management will use to evaluate the performance of the managers towards achieving the goals of IT and the Agency.

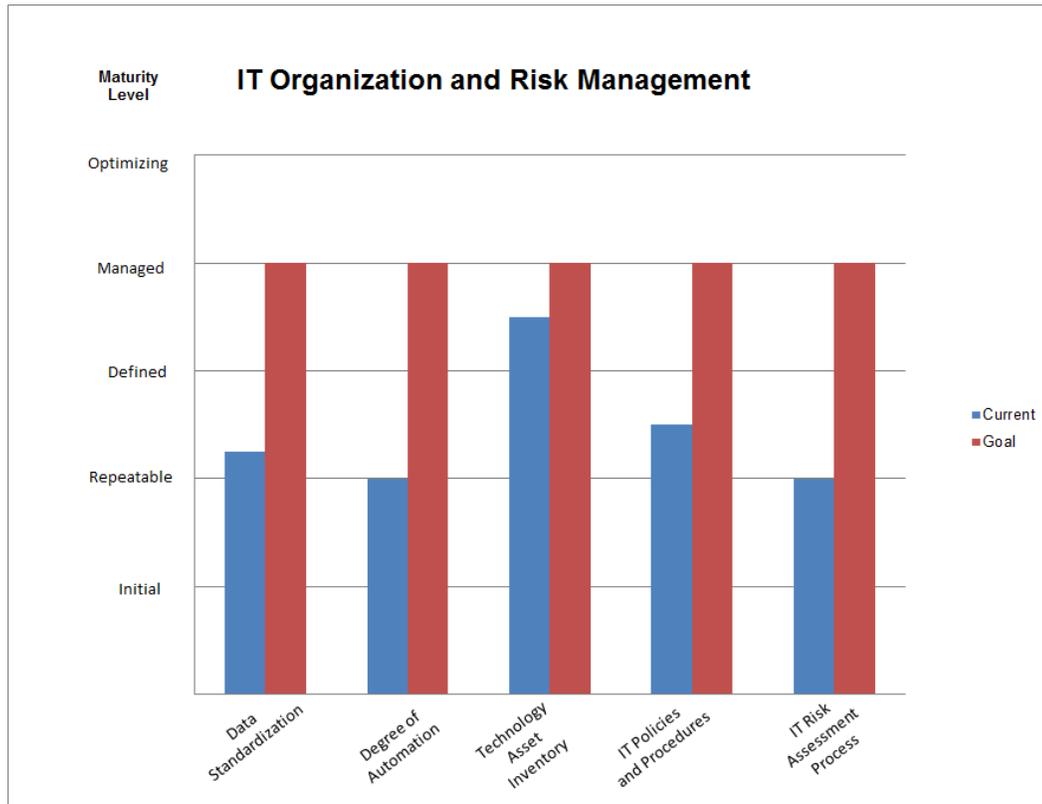
Managed: Monitor and measure the performance of IT Senior Management in alignment with the goals and responsibilities of ITS and the Agency, including incorporating specific measures into the performance evaluations of IT management that align with the strategic goals and programs of DIR.

Management Response:

DIR IT management agreed with Internal Audit's recommendations.

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

IT Organization and Risk Management



Issue 21: IT Data Governance

DIR’s data is not centrally maintained, tracked, or standardized. The data management policy and procedures document does not enforce standards on data governance.

Recommendations:

To mature the DIR IT Governance to a “Defined” or “Managed” state, DIR IT management should:

Defined: Develop a Data Management Policy that is enforceable and sensible for the Agency to facilitate more efficient data management processes and the tracking of key information.

Managed: Implement management technology solutions to reduce dependencies on file shares and other unstructured and difficult to data management methods currently in use.

Management Response:

DIR IT management agreed with Internal Audit’s recommendations.

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

Issue 22: IT Process Automation

DIR IT-related organizational processes are not integrated and automated, and require a high level of manual intervention. Processes such as Corporate Contracts - eProcurement have very limited levels of automation.

Recommendations:

To mature the DIR IT Governance to a “Defined” or “Managed” state, DIR IT management should:

Defined: Identify the processes critical to ITS and DIR, and focus on increasing the level of automation and integration of those processes. In order to improve productivity and better align organizational controls, technology solutions such as e-Procurement tools may need to be considered.

Managed: Define and automate processes within ITS and DIR that would increase operational efficiency and reduce the manual processing time required by personnel within the Agency.

Management Response:

DIR IT management agreed with Internal Audit’s recommendations.

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

Issue 23: IT Policies and Procedures

The DIR Information Technology Services (ITS) policy and procedures documents are incomplete and not maintained or updated on a periodic basis. A formal Information Security Policy is not documented. In the absence of a formalized Information Security Policy, the Agency Security Plan (Security Matrix) is used to ensure adherence to the Texas Administrative Code Chapter 202 and the National Institute of Standards and Technology (NIST) requirements. There is a section in the DIR Employee Handbook referencing the security of information resources, but a formalized stand-alone Information Security Policy does not exist. Additionally, procedures for software development, change management, and risk management are not documented.

Recommendations:

To mature the DIR IT Governance to a “Defined” or “Managed” state, DIR IT management should:

Defined: Ensure that all relevant and necessary policies and procedures are developed, documented, approved, and aligned with relevant IT governance and management frameworks such as: COBIT 5, NIST SP 800-53, ITIL, International Organization for Standardization (ISO) 27001, etc.

Formal policies for critical IT process such as: IT Development, IT Change Management, Risk Management, and Agency-wide Information Security should be developed and documented. Approval of these policies should involve the ELT of the Agency.

Managed: Carry out periodic reviews of policies and procedures to ensure the documents are up-to-date.

Management Response:

DIR IT management agreed with Internal Audit's recommendations.

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

Issue 24: IT Risk Management

There is no documented IT Risk Management Policy and procedures that define the process to proactively perform IT risk assessments and subsequent risk mitigation. IT risk identification and mitigation only occurs at a basic level as a reactive measure in response to security incidents or other identified issues resulting from tool alerts. Such incidents are normally tracked as Help Desk tickets.

Recommendations:

To mature the DIR IT Governance to a "Defined" or "Managed" state, DIR IT management should:

Defined: Develop and implement policies and procedures to proactively plan and perform IT risk assessments on a periodic basis.

Managed: Establish and maintain a comprehensive IT risk management plan that catalogues sources of IT risk, categorizes those risks based on probability and impact, prioritizes the risks based a quantifiable scoring method, and documents the management's risk mitigation strategy that can be used to monitor the status of each risk periodically.

Management Response:

DIR IT management agreed with Internal Audit's recommendations.

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

Appendix A – Objectives, Scope, and Methodologies

The scope of the audit project included the procedures to determine the maturity of the DIR's overall governance and governance specific to the Information Technology (IT) function. The scope of the audit concerned the framework and procedures implemented by the DIR Board and the Executive Leadership Team (ELT) to inform, direct, manage, and monitor the activities of the Agency, including the enterprise programs delivered by DIR in alignment with the Agency's strategic objectives. In addition, the audit team reviewed the IT governance of the Agency, consisting of the leadership, organizational structure, policies and processes that ensure the Agency's IT function supports the organization's strategic objectives. The audit did not include evaluations of the unique governance structures of individual enterprise programs of DIR. In addition, the scope of the project did not include a review of ethics, a critical component of governance because a DIR Ethics Evaluation was conducted and reported separately in Internal Audit Report No. 16-102.

Agency governance is the combination of processes and structures implemented by the Board and Executive Management to inform, direct, manage, and monitor the activities of the organization toward the achievement of its strategic objectives.

IT governance consists of the leadership, organizational structure, and other processes that ensure that the Agency's information technology supports the organization's strategic objectives.

Governance and IT governance were evaluated in two objectives against separate maturity models developed within professional frameworks from authoritative guidance and national governance associations.

Objective 1, Scope, and Methodology

Objective 1: Assess the design and operating effectiveness of DIR's governance processes.

The following elements were included in the scope of our procedures:



The elements of governance to be included in the scope of our procedures are:

- **Board Oversight**
 - Board charter of bylaws
 - Policies adopted by the Board to provide oversight to DIR
 - Board subcommittees
- **Strategy, Policies, and Procedures**
 - Agency policies and procedures
 - Mission/value statement and objectives
 - Strategic planning and direction
 - Goals
 - Performance metrics
- **Structure and Accountability**
 - Human Resources policies and procedures

- Job descriptions
- Performance evaluations
- Compensation/incentive plans
- Training/staff development plans
- Succession plans
- **Communication and Reporting**
 - Communication to Board and staff
 - Board reporting
 - Internal reporting
 - Staff meetings
 - Performance monitoring and dashboards
 - Public information
- **Assessment and Risk Management**
 - Identification and assessment of risks
 - Risk management
 - Monitoring
 - Compliance

The maturity model used to evaluate DIR's governance is documented in Appendix B. The authoritative standards and guidance set by national associations used to develop the maturity model include:

- COSO 2013 Internal Control Framework
- National Association of Corporate Directors (NACD)
- Texas Government Code, Chapter 2054
- Texas Administrative Code, Chapter 201
- DIR Board Member Guide, 2016

Objective 2, Scope, and Methodology

Objective 2: Assess whether the DIR Information Technology (IT) governance supports the Agency's strategic goals and objectives, IT resource and performance management are effective, and the risks that may adversely affect the IT function.

The following elements were included in the scope of our procedures:



The elements of IT governance to be included in the scope of our procedures were:

- **Organizational and Governance Structures**
 - Executive and IT personnel are interacting and communicating current and future needs across the organization.
 - IT governance mirrors the organization structure in its enterprise architecture should also be reviewed.
- **Executive Leadership and Support**
 - Relationship between IT objectives and the strategic needs of DIR and the ability of IT leadership to effectively communicate this relationship to DIR staff.

- Roles and responsibilities are assigned within the IT organization and how they are executed.
- **Strategic and Operational Planning**
 - Tactical operating plan is established to support strategic plan
 - IT governance methodology forecasts future needs and resources for projects
- **Service Delivery and Measurement**
 - Framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.
- **IT Organization and Risk Management**
 - Processes used by the IT organization to identify, assess and monitor/mitigate risks within the IT environment.
 - Expectations are monitored to ensure that staff have appropriate accountability for managing risk.

The maturity model used to evaluate DIR's IT governance is documented in Appendix B. The authoritative standards and guidance set by national associations used to develop the maturity model include:

- Global Technology Audit Guide (GTAG) 17 Auditing IT Governance
- COSO 2013 Internal Control Framework
- COBIT 5 Information Technology Control Framework
- Texas Government Code, Chapter 2054
- Texas Administrative Code, Chapter 201
- DIR Board Member Guide, 2016

Appendix B – Maturity Models

DIR Governance Maturity Model

DIR Governance Maturity Model					
Attribute	Initial	Repeatable	Defined	Managed	Optimized
Board Roles and Oversight Are Board roles explicitly defined through committees and charters? How consistently and effectively does the Board provide oversight to the organization?	Board does not have defined committees, a charter or bylaws and objectives have not been defined for the organization	Board has defined committees and communicated objectives and requirements for the organization	Board and its committees have established charters that been developed to align with the organization's mission and objectives	Board and its committees are functioning at the defined state building the foundation for a strong risk governance culture	Board and committees are committed to continuously improving capabilities at managed stage
Strategy, Policies and Procedures Are the strategy, goals, objectives, policies, and procedures for supporting DIR's mission clearly defined? What are the key performance measures and metrics to monitor achievement of the mission? Is the strategy communicated, documented, and aligned?	General understanding of strategic plan and vision. Policies and procedures are dependent on seasoned staff to carry out operations. No defined performance measures for evaluating achievement of mission and objectives	Informal policies and procedures exist and support strategic direction and key performance measures and metrics	Strategic plan has been developed, and key performance measures and metrics are defined. Policies and procedures are refined and documented	Strategic plan and goals are agreed upon and meaningful performance measures and metrics are in place. Policies and procedures are reviewed, revised, and communicated throughout the entity on a defined schedule. Performance metrics that align with the entity's mission are monitored	Strategic plan and goals are understood and redefined annually. Policies are continuously evaluated on an enterprise wide basis to achieve the desired risk/reward balance. Performance measures and metrics are regularly monitored and reported to management to monitor achievement of goals and objectives
Structure and Accountability How effective is the structure of the organization (Board and divisions) for managing programs, hiring, training and staff development, evaluating performance, and succession planning? Are roles and responsibilities defined with adequate staffing?	Limited accountability due to absence of clearly designated people charged with managing programs, evaluating performance, and overseeing specific risks	Responsibilities and authorities are defined for specific individuals and roles in addition to identifying staff development needs	Roles and responsibilities are clearly defined, robust management reports are utilized, key performance indicators are integrated into decision making processes, and career ladders are established	Formal lines-of-defense framework is implemented, risk measures are linked to performance goals, early warning systems are in place, capital allocation techniques are effectively deployed, and staffing levels are systematically determined	Organizational structure and delegation of authority is effective and improvement initiatives are established and are integrated with development and risk management plans

DIR Governance Assessment

DIR Governance Maturity Model					
Attribute	Initial	Repeatable	Defined	Managed	Optimized
Communication and Reporting What are types of communication used by DIR for board reporting, internal reporting, staff meetings, dashboards and public information?	Informal communication and reporting guidelines exist	Basic reporting structure in place; including board reporting, retaining meeting minutes and agendas, and consistent updates to staff	Objectives and performance metrics are integrated into enterprise wide systems, providing dashboard reporting and performance management	Formal guidelines in place for consistent and timely communication to the board, internally to staff, and the public	Entity wide reporting needs are adequately serviced and the Board periodically evaluates performance management and communication effectiveness
Assessment and Risk Management What processes are in place to monitor DIR's progress for meeting stated objectives, performance metrics, risk management, and compliance?	Monitoring goals, objectives, and compliance is informal. Risk management is fragmented and ad hoc. Individual risks are managed in silos and the organization behaves reactively to events. There is no monitoring of performance metrics	Basic risk management policy structures and processes are in place, including performing an annual risk assessment; performance goals are informally established; performance metrics are informally monitored	Evidence of risk-sensitive and risk-aware decision making; control deficiencies drive improvement initiatives; risk measures are linked to performance goals	Improved quantification, time tested models, and data analytics assist decision makers with forecasting and scenario planning analysis to identify emerging risks and anticipate potential disruptive change. Performance metrics are regularly monitored	All elements of the risk management structure fully align with business environment changes; compliance and performance goals are continuously monitored and used to analyze risk trends associated with goals and objectives

Note: Red bordered cells that begin with a * indicate the maturity goal determined by Executive Management.

DIR IT Governance Maturity Model

DIR IT Governance Maturity Model					
Attribute	Initial	Repeatable	Defined	Managed	Optimized
<p>Organization and Governance Structures To determine whether the structure of the organization and its operational components are clearly organized such that the IT function can efficiently and effectively help enable the achievement of the organization's objectives.</p>	<p>The need for IT governance is recognized, but there are no formal IT governance decision bodies (such as a technology steering committee, change approval board, etc.).</p>	<p>Decision bodies are formed, however not formalized by charters officially sanctioned by the Board. Meetings may occur on an ad hoc basis and/or have informal agendas. Communication of technology governance matters to the Board occurs on an ad hoc basis</p>	<p>* Decision bodies have established charters that align with the organization's mission and objectives and are sanctioned by the Board. The role of decision bodies with respect to IT governance is communicated and understood. Some information from the CIO and decision bodies is communicated to the Board on a defined basis, however the Board may be challenged to understand.</p>	<p>Decision bodies are integrated with the organizational and technology strategic plans. Decision bodies are ingrained with the workflow and not easily circumvented by members of management. The Board is at least partially educated and relevant information from the CIO and decision bodies is reported to the Board regularly.</p>	<p>IT strategic plan is regularly reviewed against the organizational strategic plan. Decision bodies' charters and strategic role are regularly reviewed and modified as necessary to optimize relevance. The Board is educated upon and evaluates information reported by the CIO and decision bodies on a regular basis.</p>
<p>Executive Leadership and Support To determine whether the tone at the top and executive leadership set a clear vision for the organization communicating how IT supports and enables the enterprise to achieve its objectives.</p>	<p>General understanding of IT strategic plan and vision. Policies and procedures are dependent on seasoned staff to carry out operations. The CIO is viewed as an IT role, is not necessarily part of senior leadership within the organization, and does not present information to the board.</p>	<p>Informal policies and procedures exist and support IT strategic direction. IT budgets are created and approved on an annual basis, taking strategic direction and understood key initiatives into consideration. The role of the CIO is not formally defined, but is well understood by senior management and the board. The CIO is considered a part of senior management and periodically presents information to the board.</p>	<p>*IT strategic plan has been developed, policies and procedures are aligned, documented and periodically updated. IT budget process is built based on an analysis of the defined strategic plan and key initiatives approved by decision bodies. The role of the CIO is well defined, the CIO is a member of senior management and meets regularly with the board.</p>	<p>IT strategic plan and goals are agreed upon with senior management and the Board. Policies and procedures are reviewed, revised, and communicated throughout the entity on a defined schedule. IT budget is approved by the technology steering committee or similar decision body. The role of the CIO is aligned to the organization's strategic plans. The content presented by the CIO to the board is aligned to the strategic and operating plans.</p>	<p>IT strategic plan and goals are understood and redefined at least annually. Policies are continuously evaluated on an enterprise wide basis to achieve the desired risk/reward balance. Technology trends and developments are regularly monitored and evaluated for impact against the IT strategic plan and/or affected policies and procedures. The CIO's communication to the board reflects not only alignment with the strategic and operating plans, but also forward looking considerations relating to trends and developments.</p>

DIR Governance Assessment

DIR IT Governance Maturity Model

Attribute	Initial	Repeatable	Defined	Managed	Optimized
<p>Strategic and Operational Planning To determine whether a tactical operating plan is in place and aligned with the organization's strategic plan and whether the operating plan provides the mechanism for how the IT function is measured in terms of supporting and enabling the achievement of goals defined within the strategic plan.</p>	<p>Tactical plans are not created based on the strategic direction. Performance is only measured at the highest level. IT acquisitions occur through a variety of methods. IT org structure and roles are not well defined and poorly understood.</p>	<p>Informal tactical plans are created based on the IT strategic direction. Performance measures are informally considered and evaluated. IT acquisitions go through a generally understood process and include a cost analysis. IT org structure is sufficient, but may occasionally be confusing as to roles and responsibilities.</p>	<p>*Tactical operating plans are created based on IT strategic plan. Some KPIs are defined/reviewed to measure the effectiveness of the IT function. IT investment decisions include cost benefit assessment and flow through defined decision bodies. IT organization is structured effectively relative to the size and composition of the organization.</p>	<p>Tactical operating plans based on IT strategic plan are tracked through the year. Related KPIs are broadly defined and regularly reviewed to monitor the effectiveness of the IT function. IT investment decisions include cost benefit assessment, flow through defined decision bodies, and are evaluated via post-mortem. IT organization structure is assessed and reaffirmed by appropriate decision bodies at least annually.</p>	<p>Tactical operating plans based on IT strategic plan are monitored through the year. Relevant KPIs are integrated into daily workflow, including the use of tools. IT investment decisions are evaluated formally for success / failure. IT organization structure and appropriate staffing metrics are formally monitored to ensure adequate resources are staffed for workloads.</p>
<p>Service Delivery and Measurement To determine whether IT spending is proactively managed and the resulting value as a result of IT spending is measured.</p>	<p>IT costs are not tracked within IT. Value can only be informally articulated when requested by senior management. CIO performance measures are unclear or poorly understood. Technology sourcing occurs through a variety of methods</p>	<p>IT costs are tracked within IT but not easily relatable to key initiatives or the strategic plan. Some measurement is performed against the SLA and the strategic direction. CIO performance measures consider financial and nonfinancial data. Technology sourcing occurs through generally understood but easily circumvented processes.</p>	<p>IT costs are tracked at the project level and can be related to the strategic plan. IT value and deliverables are measured against the SLA and IT strategic plan. IT costs are tracked regularly against the budget. CIO performance is measured by defined financial and nonfinancial data. Technology sourcing arrangements and processes are in place, and are measured.</p>	<p>*IT costs are proactively tracked at the project level linked to the IT strategic plan. IT value and deliverables are measured against the SLA and IT strategic plan using metrics. IT operational costs are tracked proactively against the budget. CIO performance is measured using agreed upon criteria. Technology sourcing flows through defined processes and its monitored.</p>	<p>IT costs are proactively tracked across the portfolio representing the initiatives of the strategic plan. IT value and deliverables are measured against the SLA and IT strategic plan using metrics that are regularly published to decision bodies. IT operational costs are tracked proactively against the budget. CIO performance is continually measured using a dashboard. Technology sourcing flows through defined processes and its continuously monitored.</p>

DIR Governance Assessment

DIR IT Governance Maturity Model

Attribute	Initial	Repeatable	Defined	Managed	Optimized
IT Organization and Risk Management To determine whether IT risks and resources are managed effectively.	No data inventory exists and little to no data sharing between systems. Organizational processes are not well integrated or automated, relying heavily on end user computing. Inventory of key applications and infrastructure is not well understood. IT policies and procedures are not defined and IT risk assessment is not performed.	Key data sets are understood may be shared across applications and the IT infrastructure. Organizational processes are not heavily integrated or automated, relying on end user computing. Inventory of key applications and infrastructure is dated or non-existent. IT policies and procedures are loosely defined. IT risk is informally assessed.	Key data sets are defined and shared across applications and the IT infrastructure. Organizational processes are integrated and automated, with some significant end user computing. An inventory of IT infrastructure and applications exists. IT policies and procedures consider recognized frameworks. A defined process exists for executing IT risk assessments.	*Data architecture is well defined and shared across applications and the IT infrastructure. Organizational processes are well integrated and automated, with end user computing being reserved for more complex tasks. An inventory of IT infrastructure and applications exists and is maintained. IT policies and procedures are based upon recognized frameworks. IT risk assessments are conducted annually.	Data architecture is standardized and easily shared across applications and the IT infrastructure. Organizational processes are well integrated and automated, with only limited end user computing. An inventory of IT infrastructure and applications exists and is maintained. IT policies and procedures are based upon recognized frameworks and proactively monitored for necessary updates. IT risk assessments are conducted annually and include elements of continuous monitoring through Key Risk Indicators.

Note: Red border cells that begin with a * indicate the maturity goal determined by Executive Management.

Appendix C – Management Responses

Action Plans

Planned course of action to address the recommendation.

Estimated Implementation Dates

Date on which the action plan will be finished.

Responsible Management Staff

Manager responsible for the implementation and execution of the action plan.

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
Issue 1: Charters and Bylaws			
<p>Defined: Establish formal charters or bylaws for the Board subcommittees to outline the responsibilities and reporting requirements for each body. Charters should include the following:</p> <ul style="list-style-type: none"> • Subcommittee's charge or mission statement • Authority and responsibilities of the Subcommittee • Composition of the Subcommittee • Meeting frequency • Documentation and approval of meeting minutes <p>Managed: Conduct recurring meetings with documented and approved meeting minutes for a sustained time period of six to 12 months.</p>	<p>Defined (Short-term Goal): DIR staff will draft charter documents for each DIR Board Subcommittee. The drafts will be submitted to each Subcommittee and the DIR Board chair for review. At the direction of the Board Chair, the charters will be submitted to the full Board for approval.</p> <p>Managed (Long-term Goal): See above.</p>	<p>Defined (Short-term Goal): 2/28/2017</p> <p>Managed (Long-term Goal): 2/28/2018</p>	<p>General Counsel, Office of General Counsel (OGC)</p>
Issue 2: Board Policies			

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
<p>Defined: Update Board policies to provide detailed guidance and direction on how Agency management will fulfill the statutory requirements of the Texas Government Code and the Agency’s strategic goals.</p> <p>Managed: Conduct reviews and updates of policies on a regular basis to ensure the policies are up-to-date and relevant for the Agency. Reviews should occur at least annually.</p>	<p>Defined: DIR staff will update the policies with additional guidance for compliance and route for approval through the standard rulemaking process.</p> <p>Managed: Texas Administrative Code (TAC), Title 1, Part 10, Section 201, DIR’s General Administration Rules, will be updated on a regular basis pursuant to the 4-year rule review cycle.</p>	<p>Defined: 2/28/2017</p> <p>Managed: 2/28/2021</p>	<p>General Counsel, OGC</p>
<p>Issue 3: Subcommittee Minutes</p>			
<p>Defined: Prepare and review minutes of each Subcommittee that are approved by the Subcommittee. These minutes should be retained in a central repository with appropriate access restrictions to the Board and members of the Executive Leadership Team.</p> <p>Managed: Conduct recurring meetings with documented and approved meeting minutes for a sustained time period of six to 12 months.</p>	<p>Defined (Short-term Goal): Subcommittee staff will prepare agendas, materials and minutes for each Subcommittee meeting. Minutes may consist solely of action items for staff. Documents will be retained in a collaborative site, such as SharePoint, with role based security and access.</p> <p>Managed (Long-term Goal): See above.</p>	<p>Defined (Short-term Goal): 2/28/2017</p> <p>Managed (Long-term Goal): 2/28/2018</p>	<p>General Counsel, OGC</p>
<p>Issue 4: Performance Metrics</p>			

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
<p>Defined: Identify metrics that provide meaningful information to monitor the Agency’s performance and accomplishment of the key strategic initiatives from the approved strategic plan.</p> <p>Managed: Define processes to monitor and consistently report the metrics to DIR Management and the Board. Dashboards should be developed to accurately report the outcome of the performance metrics to all applicable users.</p>	<p>Defined (Short-term Goal): DIR will identify and monitor performance metrics to measure Agency accomplishments in support of the Agency Strategic Plan.</p> <p>Managed (Long-term Goal): DIR will implement metric dashboards and regular reporting of Agency accomplishments relative to defined metrics.</p>	<p>Defined (Short-term Goal): 12/31/2016</p> <p>Managed (Long-term Goal): 8/31/2017</p>	<p>Defined (Short-term Goal):</p> <ul style="list-style-type: none"> • Chief Technology Officer (CTO) • Chief Operating Officer (COO) • Chief Financial Officer (CFO) <p>Managed (Long-term Goal):</p> <ul style="list-style-type: none"> • Executive Director • Director, Information Technology Services (ITS)/ Information Resources Manager (IRM)
Issue 5: Staff Development Plans			
<p>Repeatable: Establish a development and training plan for each employee level within DIR. The development and training plan should include continuing education for professional certification requirements and professional development training to maintain and improve the skill sets and knowledge of staff that is required to perform their job duties.</p> <p>Defined: Document the expectations for the training plans for each level of employee that include the expected number of hours of training, training budgets and expected timeframes of completion.</p> <p>Managed: Monitor the completion of the training plans to ensure that employees have current and relevant knowledge and skills for their function within the Agency.</p>	<p>Repeatable (Short-term Goal): DIR’s Human Resources Department will work with all DIR divisions to establish development and training plans for each employee within DIR. Plans will include continuing education for professional certifications as well as training to maintain and improve the skill sets and knowledge of staff required to perform their job duties.</p> <p>Defined (Short-term Goal): DIR’s Human Resources Department will work with all DIR divisions, including Budget, to develop and document requirements for training hours, budgets, and completion timeframes.</p> <p>Managed (Long-term Goal): DIR’s Human Resources Department will leverage the CAPPS Learning Management System (LMS) to facilitate the ability of supervisors to monitor the completion of training plans and notify management of deviations from plans.</p>	<p>Repeatable (Short-term Goal): 4/30/2017</p> <p>Defined (Short-term Goal): 4/30/2017</p> <p>Managed (Long-term Goal): 4/30/2018</p>	<p>Human Resources Director, CFO</p>
Issue 6: Reporting Guidelines			

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
<p>Defined: Establish and document formal guidelines and standards for Agency communications involving appropriate content for audiences and procedures to obtain approval before the release of communications to the intended user.</p> <p>Managed: Implement controls to approve and monitor communication releases to ensure communications are in accordance with established guidelines.</p>	<p>Defined/Managed (Short-term Goal): DIR will formalize the communication guidelines and obtain approval from the Executive Director. Communications guidelines will include process instructions to be shared with Agency divisions.</p>	<p>8/31/2016</p>	<p>DIR Press Secretary, Office of Public Affairs (OPA)</p>
<p>Issue 7: ELT Meeting Structure and Action Items Communication</p>			
<p>Defined: Incorporate a standing agenda into the reoccurring calendar invitation to the ELT members to provide a guideline for the direction and content and of the ELT meetings. The standing agenda would document the recurring discussion items based on their respective frequency.</p> <p>Managed: Prioritize decisions made on IT projects by the ELT and document any action items to communicate commitments and establish accountability. This documentation could occur via an email from the Executive Director, or their Administrative Assistant, to the ELT summarizing the action items or decisions made.</p>	<p>Defined (Short-term Goal): Executive Leadership Team meeting calendar invitations will contain standing and nonrecurring agenda items.</p> <p>Managed (Long-term Goal): Prioritization of IT projects and communication about action items are addressed in action plans for Objective 2 (refer to Issue 14).</p>	<p>9/1/2016</p>	<p>General Counsel, OGC</p>
<p>Issue 8: Real-time Reporting</p>			

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
<p>Defined: Design real-time or near real-time methods to monitor and report performance to the ELT and the Board, once performance metrics have been identified and established.</p> <p>Managed: Develop reporting methods that actively disseminate information to be used to make operational and management decisions. This could be accomplished by dashboards that display upon login to DIR systems, daily flash reports, or systematic notifications to personnel responsible for monitoring and executing activities that affect the metrics.</p>	<p>Defined (Short-term Goal): DIR will implement dashboard reporting of performance metrics as described in issue #4.</p> <p>Managed (Short-term Goal): DIR will deploy an alert notification process to inform key/ appropriate employees when expected results are not met.</p>	<p>8/31/2017</p>	<ul style="list-style-type: none"> • Deputy Executive Director • Director, ITS/IRM
<p>Issue 9: Agency-wide Risk Assessment</p>			
<p>Repeatable: Develop an Agency-wide Risk Assessment to assist DIR in identifying and mitigating the risks to accomplishing the mission and objectives. The Risk Assessment should consider risks that negatively affect the accomplishment of objectives and that is related to, but not limited to, operations, strategy, legislation, compliance, and financial processes.</p> <p>Defined: Determine and establish a recurring process to periodically update the Risk Assessment to ensure the assessment reflects the current risk profile of the Agency.</p>	<p>Repeatable (Short-term Goal): DIR will document an Agency-wide Risk Assessment considering risks that could result in the Agency's inability to accomplish its mission and objectives.</p> <p>Defined (Short-term Goal): DIR will develop a methodology for periodically updating the Agency-wide Risk Assessment to establish mitigation plans for high risks identified across the organization.</p>	<p>10/31/16</p>	<p>Development:</p> <ul style="list-style-type: none"> • Director, ITS/IRM • Executive Leadership Team (ELT) <p>Approval: Deputy Executive Director</p>
<p>Issue 10: Risk Management Plan</p>			
<p>Defined: Develop an Agency Risk Management Plan to mitigate risk to an acceptable level for Management and the Board, as well as monitor the risks to ensure that they do not exceed the tolerable thresholds, once DIR has implemented the Agency-wide Risk Assessment.</p>	<p>Defined (Short-term Goal): The Chief Technology Office (CTO) will develop and implement an Agency-wide Risk Assessment process and plan that will occur on a biennial basis.</p>	<p>12/31/2016</p>	<p>Development: CTO</p> <p>Support:</p> <ul style="list-style-type: none"> • Director, ITS/IRM • Information Security Officer (ISO) • ELT

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
Issue 11: IT Roles, Alignment, and Strategic Plan			
<p>Defined: Document the roles and responsibilities of Agency IT and the IT governance decision bodies and formally communicate them to all DIR employees via the internal forums such as the DIR internal portal.</p>	<p>Defined (Short-term Goal): ITS will develop an IT Governance Plan that reflects the Agency IT and IT governance roles, responsibilities, and alignment with the Agency Strategic Plan and communicate the Plan to all DIR employees.</p>	<p>11/30/2016</p>	<p>Development: Director, ITS/IRM</p> <p>Approval: Deputy Executive Director</p>
Issue 12: IT Succession Planning			
<p>Defined: Document a well-defined Succession Plan for the key leadership positions that includes the name of the successor and that provides guidance, training, information, and the tools needed to support a successful succession.</p>	<p>Defined (Short-term Goal): Succession plans will be constructed to include the successor roles and will include training and tools necessary to ensure the succession plans are viable.</p>	<p>3/31/2017</p>	<p>Development: Director, ITS/IRM</p> <p>Approval: Deputy Executive Director</p>
Issue 13: IT Strategic Plan			
<p>Defined: Create an IT Strategic Plan that defines the ITS's strategy for helping DIR fulfill the Agency's overall Strategic Plan. Alternatively, this could be accomplished as an appendix to the existing Agency Strategic Plan. This should include the mechanism for how ITS is measured in terms of supporting and enabling the achievement of goals defined within the Strategic Plan. It should also establish the foundation for quantifiable performance measures that help demonstrate the true value provided by ITS.</p>	<p>Defined (Short-term Goal): The Director of ITS will develop an IT Strategic Plan that defines the ITS's strategy for accomplishing the Agency's overall Strategic Plan. It will establish the foundation for quantifiable performance measures that help demonstrate the value provided by ITS.</p>	<p>12/31/2016</p>	<p>Development: Director, ITS/IRM</p> <p>Approval: Deputy Executive Director</p>
Issue 14: IT Goal Prioritization Support			

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
<p>Defined: Define the assessment parameters for determining the Agency’s top priority goals and retain documentation on goals selection and assessment results. ELT meetings on the prioritization of goals should be documented for transparency and accountability purposes.</p>	<p>Defined (Short-term Goal): Assessment parameters of the Agency’s top project goals will be documented. Assessment results, (initial and changes) from ELT meetings will be captured by the Deputy Executive Director (or COO) and documented within each project record.</p>	<p>9/1/2016</p>	<p>Development and Approval:</p> <ul style="list-style-type: none"> • Deputy Executive Director • COO • Project Management Officer (PMO)
<p>Issue 15: IT Change Management Approval Guidelines</p>			
<p>Defined: Establish documented guidance on the type of projects that are required to be discussed in the Change Management meetings. The guidance should include specifications for the types of information to submit to the CCB including details on the size of the projects (in terms of hours), cost, the type of project, relationship to strategic and tactical plans, and any other criteria the CCB may consider beneficial for decision making purposes.</p>	<p>Defined (Short-term Goal): ITS will work with the PMO to document change management guidance including specifications for the types of information to submit to the CCB including details on the size of the projects (in terms of hours), cost, the type of project, relationship to strategic and tactical plans, and any other criteria the CCB may consider beneficial for decision making purposes.</p>	<p>2/28/2017</p>	<p>Development: Director, ITS/IRM</p> <p>Approval: Deputy Executive Director</p>
<p>Issue 16: IT Performance Metrics</p>			
<p>Defined: Define KPIs that measure the effectiveness of ITS based upon Service Level Agreements (SLAs) and key strategic and tactical plans. The KPIs should be measured on a periodic basis to ensure that ITS’s performance is meeting Agency requirements.</p>	<p>Defined (Short-term Goal): ITS will develop quantifiable measurements for the activities that the ITS team conducts in service to the Agency.</p>	<p>1/31/2017</p>	<p>Development: Director, ITS/IRM</p> <p>Approval: Deputy Executive Director</p>
<p>Issue 17: IT Project Prioritization</p>			

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
<p>Defined: Ensure that any action items and prioritization decisions of IT projects made in the ELT meetings are documented to communicate the commitments and establish accountability. A detailed cost-benefit analysis should be performed to quantify the expected project results. The prioritization of projects should be based on this numerical assessment of the cost-benefit analysis/Return on Investment (ROI), along with other criteria as deemed appropriate by the ELT.</p>	<p>Defined (Short-term Goal): The IRM will work with the ELT representatives and business units to capture criteria relevant to prioritization within IT Services and the ELT.</p>	<p>6/30/2017</p>	<p>Development:</p> <ul style="list-style-type: none"> • Director, ITS/IRM • Stakeholder Management Team <p>Approval: Deputy Executive Director</p>
<p>Issue 18: IT Resource Planning</p>			
<p>Defined: Document its resource planning process. The process should describe how the current and forecasted future resource requirements are considered and planned, including options for resourcing and sourcing strategies.</p>	<p>Defined (Short-term Goal): DIR will document the process that is in practice today, including the methodology that is followed to perform resource planning and principles that optimally meet the Agency needs.</p>	<p>12/31/2016</p>	<ul style="list-style-type: none"> • Deputy Executive Director • COO with support of PMO
<p>Issue 19: IT Post-Implementation Evaluation</p>			
<p>Defined: Pre-define and communicate the targets and criteria against which the success of a project will be evaluated. Targets should include budgetary and cost-benefit goals.</p> <p>Managed: Ensure that projects are evaluated post implementation to compare their results and quality with pre-defined success targets. Such evaluations should also include analysis of actual budget results against those included in the initial cost-benefit. Lessons learned should be documented and factored into future IT investment decisions.</p>	<p>Defined (Short-term Goal): DIR will document and implement defined project targets and criteria, including budgetary and cost-benefit goals that will be used to determine project success consistently.</p> <p>Managed (Short-term Goal): DIR will implement post-implementation project evaluations and record the evaluations results in Innotas as part of the official project record.</p>	<p>Defined (Short-term Goal): 1/31/2017</p> <p>Managed (Short-term Goal): 4/30/2017</p>	<p>Development: Director, ITS/IRM</p> <p>Approval: Deputy Executive Director</p>
<p>Issue 20: IT Performance Evaluations</p>			

DIR Governance Assessment

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
<p>Defined: Pre-define and communicate the criteria to include in the evaluations IT Senior Management will use to evaluate the performance of the managers towards achieving the goals of ITS and the Agency.</p> <p>Managed: Monitor and measure the performance of IT Senior Management in alignment with the goals and responsibilities of ITS and the Agency, including incorporating specific measures into the performance evaluations of IT management that align with the strategic goals and programs of DIR.</p>	<p>Defined (Short-term Goal): ITS will define and communicate performance criteria as part of the new goal based employee evaluation process being implemented by Human Resources.</p> <p>Managed (Short-term Goal): ITS will participate in the goal based performance management process, which incorporates Agency strategic goals for all employees to align individual goals against.</p>	<p>9/30/2016</p>	<p>Development: Director, ITS/IRM</p> <p>Approval: Deputy Executive Director</p>
<p>Issue 21: IT Data Governance</p>			
<p>Defined: Develop a Data Management Policy that is enforceable and sensible for the Agency to facilitate more efficient data management processes and the tracking of key information.</p> <p>Managed: Implement management technology solutions to reduce dependencies on file shares and other unstructured and difficult to data management methods currently in use.</p>	<p>Defined/Managed (Short-term Goal): ITS personnel will work with the Statewide Data Coordinator (SDC) and DIRs Records Management Officer to develop a Data Management Policy and set of Procedures to manage DIR data within the guidelines of DIRs Records Retention Model and Data Management best practices as designed by the SDC.</p>	<p>5/31/2017</p>	<p>Development: DBA and Management Team, ITS</p> <p>Monitor: Director, ITS/IRM</p> <p>Approval: Deputy Executive Director</p>
<p>Issue 22: IT Process Automation</p>			
<p>Defined: Identify the processes critical to ITS and DIR, and focus on increasing the level of automation and integration of those processes. In order to improve productivity and better align organizational controls, technology solutions such as e-Procurement tools may need to be considered.</p> <p>Managed: Define and automate processes within ITS and DIR that would increase operational efficiency and reduce the manual processing time required by personnel within the Agency.</p>	<p>Defined (Short-term Goal): ITS recently completed an Agency Automation Assessment (“AAA”) project to determine the extent of automation needs. This process will be repeated each biennium. Analysis of the needed automation is underway.</p> <p>Managed (Short-term Goal): ITS will automate business processes where and when opportunities for increased efficiencies are identified.</p>	<p>8/31/2016</p>	<p>Development: Director ITS/IRM</p> <p>Approval: Deputy Executive Director</p>

Recommendation	Action Plan	Estimated Implementation Date	Responsible Management Staff
Issue 23: IT Policies and Procedures			
<p>Defined: Ensure that all relevant and necessary policies and procedures are developed, documented, approved, and aligned with relevant IT governance and management frameworks such as: COBIT 5, NIST SP 800-53, ITIL, International Organization for Standardization (ISO) 27001, etc. Formal policies for critical IT process such as: IT Development, IT Change Management, and Agency-wide Information Security should be developed and documented. Approval of these policies should involve the ELT of the Agency.</p> <p>Managed: Carry out periodic reviews of policies and procedures to ensure the documents are up-to-date.</p>	<p>Defined (Short-term Goal): DIR will perform a gap analysis of all relevant and necessary policies and procedures as they map to NIST SP 800-53 and ITIL version 3.</p> <p>Managed (Short-term Goal): DIR will perform a biennial review of the policy and procedure mapping.</p>	<p>6/30/2017</p>	<p>Delivery by: ISO</p>
Issue 24: IT Risk Management			
<p>Defined: Develop and implement policies and procedures to proactively plan and perform IT risk assessments on a periodic basis.</p> <p>Managed: Establish and maintain a comprehensive IT risk management plan that catalogues sources of IT risk, categorizes those risks based on probability and impact, prioritizes the risks based a quantifiable scoring method, and documents the management's risk mitigation strategy that can be used to monitor the status of each risk periodically.</p>	<p>Defined/Managed (Short-term Goal): Refer to Issue #10. ITS will participate in the biennial Agency Risk Assessment.</p> <p>Managed (Short-term Goal): ITS will document sources and probabilities of IT risk and perform a biennial review.</p>	<p>Defined/Managed (Short-term Goal): 12/31/2016</p> <p>Managed (Short-term Goal): 8/31/2017</p>	<p>Development: CTO</p> <p>Support:</p> <ul style="list-style-type: none"> • Director, ITS/IRM • ISO • ELT <p>Monitor: Project Coordinator, ITS</p> <p>Escalation Point: IRM</p>

Appendix D – Report Distribution

Internal Report Distribution

- Department of Information Resources (DIR) Executive Director
- DIR Deputy Executive Director/ Texas Chief Information Officer
- DIR General Counsel's Office
- DIR Public Affairs Office
- DIR Chief Procurement Office
- DIR Chief Financial Officer
- DIR Chief Operations Officer
- DIR Chief Information Security Office
- DIR Chief Technology Officer
- DIR Statewide Data Coordinator

External Report Distribution

- Texas Office of the Governor
- Texas Legislative Budget Board
- Texas State Auditor's Office
- Texas Sunset Advisory Commission