

Assessing IT Governance



SHARING APPROACHES TO COMPLY WITH IIA Standard 2110.A2 (IIA -IPPF, January 2009)



Agenda



Requirements &
Resources

Larry Douglas

Texas Parks &
Wildlife
Experience

Carlos Contreras

Teacher
Retirement System
Experience

Amy Barrett

Recap

Jan Engler

Q & A
and
Discussion

Overview



**Texas Department of Insurance
(TDI)**

Larry Douglas, Project Manager

The Why



- **The Institute of Internal Auditors (IIA) established a conceptual framework to provide authoritative guidance for two distinct categories:**
 - **Mandatory** – required and necessary for the continued professional practice of auditing
 - **Strongly recommended** – provides practices for the effective implementation of : 1) Definition of Internal Auditing; 2) Code of Ethics; and 3) Standards

Source: IIA-IPPF, January 2009

Standard 2110 – Governance



2110 – Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

2110.A1 - The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.

2110.A2 - **The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.**

2110.C1 - Consulting engagement objectives must be consistent with the overall values and goals of the organization.

Performance Standard 2110.A2



“The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization’s strategies and objectives.”

Larry’s Interpretation: Does the organization’s IT infrastructure align and sustain business processes to properly manage the long-term goals for the organization?

What is IT Governance?



- **Board and Executive Management**
- **Planning**
- **Investment**
- **Resource Management**
- **Monitoring/Reporting**
- **Continuous Improvement**



Assessment of IT Governance



- **Board and Executive Management**
 - Tone at the Top – Strategic Planning
 - Organization and Reporting Structure
 - Policies and Procedures
 - Roles and Responsibilities



Assessment of IT Governance



- **Planning**

- Technical Infrastructure Roadmap
 - ❖ Objectives for IT Services
 - ❖ Details plans for all IT projects
 - ❖ SWOT Analyses
 - ❖ Resource requirements

Assessment of IT Governance



- **Investment**

- Identification of Resources
- Budget Requirements
- In-house development vs. Commercially purchased
- Alignment with Current and Future Business Needs

Assessment of IT Governance



- **Resource Management**
 - IT Steering Committees
 - Independent Verification & Validation (IV & V)
Vendor
 - ❖ Are projects properly managed?
 - ❖ What obstacles are hindering progress?
 - ❖ What options are available to redirect project back on course?
 - ❖ Should we “scrap it and restart”?

Assessment of IT Governance



- **Monitoring and Reporting**
 - Reporting policies and protocols
 - Performance matrices (PERT, Gantt)
 - Gap analyses
 - Indicators or Warning Signs
 - Compliance with original design specifications and requirements
 - Training/User Acceptance Testing

Assessment of IT Governance



- **Continuous Improvement**
 - Periodic Assessments
 - Best Practices
 - Ongoing Security Awareness
 - Succession Planning

Tools and Resources Links



- **IIA Standards:**

<http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/standards-items/index.cfm?i=8267>

- **IIA Auditing IT Governance:**

<http://www.theiia.org/bookstore/product/it-auditing-it-governance-1273.cfm>

- **IIA GTAG Guidance:**

<http://www.theiia.org/guidance/standards-and-guidance/ippf/practice-guides/gtag/gtag1/>

Tools and Resources Links



- **IT Governance Institute:**
<http://www.itgi.org>
- **ISACA:**
<http://www.isaca.org>
- **ISACA IS Auditing Guidelines on IT Governance, Document D18:**
<http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=18562>
- IT Governance Questionnaire
- IT Governance Handout

How We Did It (or are doing it)

**Texas Parks and Wildlife Department
(TPWD)**

**Carlos Contreras,
Internal Audit Director**

Present Methodology

Our present methodology utilizes the IT Governance tool including the sections on technical and operational controls.

- Interviews with:
 - Commission members
 - Executive management
 - IT management & operational staff
- Review of supporting documentation & strategic plans

Current State



- IT became a stand-alone division in 2005
- Member of executive management team
- IRM access to Executive Director
- Compliance issues due to decentralization or confusion
- “Compliance through negotiation”

Top Level Concerns



Commission (appointees) have concerns on a more strategic level

- Revenue generation
- Education/outreach
- Constituent contact



Preliminary Observations:

- Awareness of specific roles & responsibilities tied to IT governance decrease moving from operational management through executive management to the Commission.
- We found that the Commission and executive management are becoming increasingly aware of agency governance issues in the past year.

What's Changing:



- Land & Water Use Plan (Plan) contains requirements to integrate IT strategic objectives
- Tie from IT strategic objectives to overall plan
- Divisional operating plans tie to IT strategies

Governance Tools/Processes:



Governance tools/processes used by management:

- IT Steering Committee composed of Deputy Executive Directors (DEDs)
- Use of DEDs as sponsors of IT projects
- IT Project Management Office (PMO) controls from their perspective until project or phase is approved

Primary Control Areas:

- **Planning:** Only to Exec level; Data Consolidation Services (DCS) issues
- **Investment:** Adequate
- **Resource Management:** Staff constraints for internal system development; DCS issues
- **Monitoring and Reporting:** Adequate
- **Continuous Improvement:** Adequate

Operational Controls:

- **Security** – Adequate controls at this level overall; no on-going Security Awareness program.
- **Asset management** – Adequate controls
- **Project management** – Adequate controls
- **Data management** – Adequate controls
- **Infrastructure/mapping** – Adequate controls

Technical Controls:

- **Automated controls** – Adequate controls
- **Data management** – Adequate controls
- **Change control** – Inconsistent use of supporting documentation for changes including approvals.



Take Aways



- Gain an understanding of the standard
- Know your audience – approach is critical
 - Explain the process to all management levels
- Use tool as starting point & adjust accordingly
- Ensure results are effectively communicated
- Be ready to educate & create awareness

How We Did It (or are doing it)



Teacher Retirement System of Texas (TRS)

Amy Barrett, Chief Audit Executive

Entity Risk Assessment



- Old legacy systems identified as high risk via ERM
- History of system implementation failures
- Lack of discussion of current and future technology initiatives at governance level
- Strategic plan without an IT strategy
- IT governance concept not understood
- Inconsistent change management process

Current State of IT Governance



- Information Resources Steering Committee (IRSC)
- Application Programming Advisory Committee (APAC) and the Change Request Form
- Technology and Operations Workgroup (TOW)

Audit Plan Development



- **Discussion with Executive Council (EC)**
 - What is IT governance?
 - Why is Internal Audit auditing strategic risks?
- **IIA Requirement to Address IT Governance**
 - The Institute of Internal Auditors, International Professional Practices Framework (IPPF)-January 2009, IIA Standard 2110.A2

Project Goals



- Educate Board and Staff on the definition of IT governance
- Communicate current status of technology to the TRS Board



Project Approach



- Audit versus Consulting
- Outsourced to consultants
 - Other perspectives
 - True consultants
 - Greater independence
- Criteria: Information Technology Infrastructure Library (ITIL)

Process



- Gartner survey
- Risk Assessment (72/80)
- Resource management
- Change management
- Meetings
- Reviewed documents



Observations & Recommendations



● Strategy

- Strategic goals not articulated in formal strategic plan
- Strategic goals do not give specific consideration to technology requirements
- Staff resources focused on maintenance and not available to support strategy

Observations & Recommendations



- **Resources**

- Technical Architect (TA)
- Project Management Office (PMO)
- Business Analysts (BA)

Observations & Recommendations



- **Change Management**
 - IRSC: Eliminate and implement a true steering committee
 - APAC: Review all changes

Audit Committee Presentation



- **Coordinated Effort –**
 - Round table discussion with Audit Committee members, Management, Internal Audit, and Consultants
 - Future updates/discussions planned

Take Aways



- Study IT governance and be able to articulate an approach
- Tailor approach to the organization
- Tie project to IIA requirement
- Timing: Tie Project to Strategic Planning and Budget Cycle
- Plan for follow-up work

Recap



IIA Standards

IT
Governance
Resources

Educate and
Plan

Assess &
Communicate

Follow-up

Questions/Discussion?

“Progress Through Sharing”

