Illinois Tollway

Internal Audit Activity
Update

April 17, 2013

Agenda

- Internal Audit (IA) purpose, authority and responsibility
- State Internal Audit Advisory Board (SIAAB)
- Fiscal Control and Internal Auditing Act (FCIAA)
- Internal Audit activity
- External Audit
- Payment Card Industry (PCI) annual assessment
- Internal Audit resources

Illinois Tollway

IA Purpose, Authority and Responsibility

- Perform engagements proficiently and with due professional care pursuant to applicable standards
- Examine and evaluate the Tollway's policies, procedures and systems
- Ensure the reliability and integrity of information, compliance with policies, plans, laws and regulations
- Safeguarding of Tollway assets
- Ensure the economical and efficient use of resources

IA Purpose, Authority and Responsibility

The Tollway Internal Audit function has:

- Full and free access to the audit committee
- Unrestricted access to the Tollway's records, documents, property and personnel
- Authority to discuss initiatives, policies and procedures regarding risk assessment, internal controls, compliance, financial reporting and governance processes with management and other corporate governance participants

State Internal Audit Advisory Board (SIAAB)

Requirements:

- Every five years complete a quality assurance review accepted by SIAAB
- Must complete an internal quality assurance review if:
  - Internal Audit standards change
  - There is a significant change in audit personnel
- Continuing professional education

Fiscal Control and Internal Auditing Act (FCIAA)

FCIAA Requirements include:

- Two-year audit plan
- Cycle audits
- Special audits/vendor audits
- System pre-implementation reviews
- Agency certification letter to Auditor General

Fiscal Control and Internal Auditing Act

Evaluating internal controls is one of Internal Audit's primary responsibilities

Control is any action taken by management, board and other parties to manage risk and increase likelihood that established objectives and goals will be achieved

What is a cycle audit?

Audits required by FCIAA of major systems of internal accounting and administrative control conducted on a periodic basis so that all major systems are reviewed at least once every two years

Fiscal Control and Internal Auditing Act

2013 Cycle Audits

- Agency management and oversight
- Personnel and payroll
- Expenditure control
- Purchasing and procurement
- Petty cash (if FY2013 disbursements exceed $5,000)

Internal Audit Activity

Cycle Audit	2012 Audit Findings	2010 Audit Findings
Revenues and receivables	-	-
Grant administration	-	-
Property, equipment and inventory	-	-
Electronic data processing	-	-
Administrative supportive services	-	-
Budgeting, accounting and reporting	-	-
Additional Audit	**2012 Audit Findings**	
Kronos upgrade implementation	-	n/a
Total	0	0

Illinois Tollway

Internal Audit Activity

Other 2012 Activity

- Annual certification letter
- Inventory consulting review
- External audit coordination
- PCI audit coordination
- Contract and vendor audits

Internal Audit Activity

2013

- Annual certification letter
- External audit coordination
- Cycle audits
- Oases fuel audit
- Construction practices review and audit services
- Contract and vendor audits
- PCI audit coordination

External Audit

- External auditors are on site performing fieldwork
- The review includes the financial statement, compliance and Information Systems audit
- Internal Audit is the lead department coordinating the External Audit with Finance and Information Systems
- External Audit report is scheduled for release by June 30, 2013

Payment Card Industry (PCI) Annual Assessment

Compliance relates to infrastructure security and business procedures supported by Qualified Security Assessor (QSA)

- Annual self-assessment questionnaire
- Annual on-site security audit

- Mandatory compliance program resulting from a collaboration between the credit card associations
- Creates common industry security requirements for cardholder data

Payment Card Industry (PCI) Annual Assessment

- Common auditing and scanning procedures
- Facilitates broad adoption of consistent data security measures
- Annual report on information security controls surrounding payment card transactions - Tollway reached Tier 1 status in June 2012 with payment card service providers (*See Appendix A & B)*
- Required documents: Report on Compliance and Attestation on Compliance
- Report deadline: September 26, 2013

Illinois Tollway

Payment Card Industry (PCI) Annual Assessment

- Internal Audit Chief and Internal Auditor are certified as Internal Security Assessors to assist with PCI compliance assessment
- Tollway seeking to procure a five-year contract with a external firm to provide ongoing annual PCI assessment and reporting

Internal Audit Department - Resources

Cassaundra Rouse	Chief Internal Auditor
Vacant	IA Manager
Michael Pustelnik	Internal Auditor
Chad Hayden	Internal Auditor
Aldrenza Wright	Internal Auditor
Art Lemke	Information Systems Auditor

Appendix A: Levels of Merchants

Tier	Transactions per Year	Types of Targets
1	➢More than 6 million ➢Anyone with breach	Merchants, merchant agents, processors, direct connects
2	➢1 - 6 million	Merchants, merchant agents, processors
3	➢20,000 - 1 million	eCommerce merchants
4	➢All other merchants	Merchants

Appendix B: Validation Requirements

- **Level 1- Visa/MasterCard -** Annual on-site review by merchant's ISA internal auditor or a **Qualified Security Assessor** (QSA) and a quarterly network security scan with an **Approved Scanning Vendor** (ASV). Completion of a Report on Compliance (ROC) and Attestation of Compliance (AOC).
- **Level 2 -** Completion of PCI DSS Self Assessment Questionnaire annually **and** quarterly network security scan with an approved ASV.
- **Level 3 -** Completion of PCI DSS Self Assessment Questionnaire annually **and** quarterly network security scan with an approved ASV.
- **Level 4 -** Completion of PCI DSS Self Assessment Questionnaire annually **and** quarterly network security scan with an approved ASV.
- Submit summary of PCI compliance plan, via acquirer designated date.