INTEGRATED PROCESS BASED IT AUDIT USING QUALITY AND INFORMATION SECURITY MANAGEMENT SYSTEMS

ASHIT DALAL, CRISC, CGEIT, CISM, CISA, CPEA, CSSA
Managing Consultant and Vice President- Enterprise Risk Advisory Services
eDelta Consulting, Inc.
New York, NY (USA)
Ashit Dalal is the independent managing consultant and vice president of the NYC based Consulting and CPA Firm called eDelta Consulting, and is responsible for GRC, business and information security advisory services including SOC-1 and SSAE 16 practice at the global level.

With over three decades of manufacturing, consulting, auditing and training experience in wide range of industries, he currently leverages his business and finance knowledge and expertise to ensure alignment of IT with business for his clients. He also advises his clients in the areas of information security, IT audit, green business and IT strategy, IT compliance, risk management and governance. His areas of expertise include compliance and management system assessments, internal controls and IT governance, IT strategy, green IT and energy/environmental management, SCADA security and critical infrastructure protection.
Disclaimer...

The views expressed here are my personal views and not those of my company. The presentation is for education and training purpose and should not be used for any commercial purpose and monetary benefits.
Agenda

• Introduction to Process (Turtle Diagram) and Process based Auditing
• What is integrated IT audit?
• What are the key requirements to do integrated IT / IS Audit based on ISO 9001 and ISO 27001 System requirements?
• “Data Center Audit” - Case Study discussion
• Use of Integrated IT Audit Methodology to ensure and demonstrate compliance with contractual and regulatory requirements like SAS-70, COBIT, PCI-DSS etc.
• Key Benefits of integrated IT Audit approach
• Exercise & Q &A
What is Process?

Any activity using resources and managed in order to enable transformation of input into outputs can be considered as Process.
TURTLE DIAGRAM

With WHAT?
(EQUIPMENT/INSTALLATIONS)

INPUT
Customer Who has a Need

PROCESS

HOW?
(INSTRUCTIONS, PROCEDURES, METHODS)
INCLUDING SUPPORT PROCESSES

With WHO?
TRAINING KNOWLEDGE SKILLS

OUTPUT
Customer Who has a Need Met

Start With
Performance

©2012 ISACA. All Rights Reserved
Follow us @ISACANews
#NACACS
Based on PDCA Approach

Start

ACTION

PLAN

CHECK

DO

Progress
CONTINUAL IMPROVEMENT OF THE QUALITY MANAGEMENT SYSTEM

CUSTOMER

Requirements

Resource management

Management Responsibility

Measurement, analysis & improvement

Product realisation

Product or service

Value-adding activities

Information flow

CUSTOMER

Product realisation
PDCA Model for ISO27001

**Act**
- Measure Performance of the ISMS
- Identify Improvements in the ISMS and effectively implement them.
- Take appropriate corrective & preventive action
- Communicate the results and actions and consult with all parties involved.
- Revise the ISMS where necessary

**Plan**
- Define ISMS Scope and Policy
- Initial System Study
- Define a systematic approach to risk assessment
- Identify the risk
- Apply the systematic approach for assessing the risk
- Identify and Evaluate options for the treatment of risk.
- Select Control Objectives and Control the treatment of risks.

**Do**
- Implement a specific management program
- Implement controls that have been selected
- Manage Operations
- Manage Resources
- Implement Procedures and Other Control Processes

**Check**
- Undertake regular reviews of the effectiveness of the ISMS
- Review the level of residual risk and acceptable risk
- Execute the management procedure
- Undertake a formal review of its ISMS on a regular basis
- Record and report all actions and events

**Inputs**
- Define the required inputs for the ISMS

**Outputs**
- Ensure that the revision achieve their intended objectives.
PDCA Process

INTERESTED PARTIES

ISMS PROCESS

MANAGEMENT RESPONSIBILITY

PLAN
Establish ISMS

DO
Implement & Operate the ISMS

ACT
Maintain & Improve

CHECK
Monitor & Review ISMS

INFORMATION SECURITY REQUIREMENTS & EXPECTATIONS

MANAGED INFORMATION SECURITY

PDCA

P

D

C

A

PROCESS

ISO 27001

security

2012 ISACA. All Rights Reserved

4/29/2012

Follow us @ISACANews

#NACACS

Mohan Kamat
Integrated Audit Approach

- ISO 27001:2005
- COBIT 4.1
- ISO 9001:2008

Pyramid:
- Principles
- Policy
- Process
- Standards
- Architecture
- Product
- Physical Site
What are the main gaps associated with current IT Audit Methodology

Most IT Audit methodologies used today do not focus or measure the Effectiveness of Process Audited. For e.g. Change Management or Service Delivery.

Focus is mainly on compliance and not so much on process effectiveness.

Most Audits performed are Checklist-driven audits. While Checklists are good Audit Aids, but cannot help you do a Process based Audit.
Evaluating and Measuring Effectiveness

- How do you know you are doing a good job?
- How do you know you are doing the right job?

Takes a balance of measures:

- Customer (Contractual)
- Financial (Statutory)
- Internal Work Processes
- Learning & Growth
What is Effectiveness?

Extent to which planned activities are realized and planned results achieved

(Reference ISO 9000 Quality management systems – Fundamentals and Vocabulary)

Like CMM, it may be a good idea to define and measure the Maturity Level of Process Effectiveness.

How do we do it? (See next slide......)
Process Effectiveness Maturity Model

- **LEVEL: 1** - Process not implemented; planned results are not achieved.

- **LEVEL: 2** - Process implemented; planned results are not achieved and appropriate actions not taken.

- **LEVEL: 3** - Process implemented; planned results are not achieved, but appropriate actions being taken.

- **LEVEL: 4** - Process implemented; planned results are achieved.
Use of Process Effectiveness Assessment Report (PEAR) Tool / Form

• PEAR is a Process Effectiveness Assessment Report.
• It is a Process Effectiveness Measurement & Reporting Tool.
• The concept is derived from Aerospace Quality System Audit but can be effectively used for **Process based IT Audits**.
• It comprehensively describes the following:
  – Key Process Inputs
  – Key Process Outputs
  – Key Process Activities
  – Key Personnel Involved / Audited
  – Observations and Audit trail recording Section
  – Process effectiveness measurement & reporting Section
Types of Metrics

- Process Effectiveness – doing things right. (measure quality)
- Staff Productivity – people doing more things. (measure output / volume)
- Cycle Time – transaction time. (measure process efficiency)
- Staff Efficiency – people doing things faster. (people / transaction / time)
- Cost Effectiveness – transaction costs. (cost / activity)
Process Effectiveness Metrics

“doing things right”

Key Elements:
• Activities
• errors

Examples:
• Acct request errors
• Remediation errors
• False alarm rate
• Policy exceptions

Source: Spire Security 2004
CASE STUDY – 1

- Reputed Organization with HQ in VA and providing IT Services to reputed Private Sector and Government (Federal) clients.
- Small Data Center with CO-LOC facility on the East Coast.
- ISO 9001: 2008 (QMS) and ISO 20000-1 (ITSM) certified.
- Successfully deployed Integrated Management System (ISM) comprising QMS, ITSM and ISMS.
- Several common processes across all Three Systems and are given in the next Section.
- Integrated Process based and Risk based Audit approach.
## Case Study – 1

<table>
<thead>
<tr>
<th>Standard</th>
<th>ISMS</th>
<th>QMS</th>
<th>ITSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Resource Management (HR)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Corrective Action / Preventive Action</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Document Control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Records Control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Infrastructure &amp; User Access Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Contractual / Statutory and Legal Requirements (Compliance Management)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
RACI CHART

RACI denotes **Responsible (R), Accountable (A), Consulted (C) and Informed (I)**, which are four parameters used in a matrix used in decision making.

<table>
<thead>
<tr>
<th>PROCESS</th>
<th>MANAGING DIRECTOR</th>
<th>CIO</th>
<th>ISMS / QUALITY MANAGER</th>
<th>DIRECTOR HR</th>
<th>DIRECTOR FINANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR</td>
<td><strong>A</strong></td>
<td><strong>I</strong></td>
<td><strong>C</strong></td>
<td><strong>R</strong></td>
<td><strong>I</strong></td>
</tr>
<tr>
<td>CHANGE MANAGEMENT</td>
<td><strong>C</strong></td>
<td><strong>A</strong></td>
<td><strong>R</strong></td>
<td><strong>I</strong></td>
<td><strong>C</strong></td>
</tr>
<tr>
<td>RISK MANAGEMENT</td>
<td><strong>A</strong></td>
<td><strong>R</strong></td>
<td><strong>C</strong></td>
<td><strong>I</strong></td>
<td><strong>C</strong></td>
</tr>
<tr>
<td>USER ACCESS MANAGEMENT</td>
<td><strong>I</strong></td>
<td><strong>R</strong></td>
<td><strong>C</strong></td>
<td><strong>C</strong></td>
<td><strong>A</strong></td>
</tr>
<tr>
<td>COMPLIANCE MANAGEMENT</td>
<td><strong>A</strong></td>
<td><strong>R</strong></td>
<td><strong>I</strong></td>
<td><strong>C</strong></td>
<td><strong>C</strong></td>
</tr>
</tbody>
</table>
## Key Performance Indicators for various Processes

<table>
<thead>
<tr>
<th>PROCESS</th>
<th>KEY PERFORMANCE INDICATOR (KPI)</th>
<th>TARGET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Management</td>
<td>No. of Unauthorized Changes to IT Systems per quarter</td>
<td>Zero</td>
</tr>
<tr>
<td>Help Desk</td>
<td>Resolution time for Priority 1 requests</td>
<td>4 hours (Response time 30 minutes)</td>
</tr>
<tr>
<td>User Access Management</td>
<td>% of Users with Role based Access</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>No. of Active User Accounts of the Users who have left or have been transferred</td>
<td>Zero</td>
</tr>
<tr>
<td>IT Infrastructure Security</td>
<td>No. of Unpatched Servers (tracked weekly)</td>
<td>Zero</td>
</tr>
<tr>
<td></td>
<td>No. of End point devices without updated AV definitions / signatures (tracked daily)</td>
<td>Zero</td>
</tr>
<tr>
<td>Security Incident</td>
<td>No. of Physical Access Violations (tracked daily and reported weekly)</td>
<td>Zero</td>
</tr>
<tr>
<td></td>
<td>No. of Password Policy violations (tracked and reported weekly)</td>
<td>Zero</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>% Audits completed in a Quarter as per the plan</td>
<td>At least 95%</td>
</tr>
<tr>
<td>Customer Satisfaction</td>
<td>Customer Satisfaction as measured on a scale of 1 to 5 (5 highest and 1 lowest)</td>
<td>At least 4</td>
</tr>
</tbody>
</table>
Turtle Diagram - Change Management Process

With WHAT?
IT Infrastructure

With WHO?

INPUT
Customer Who has a Need

OUTPUT
Customer Who has a Need Met

REQUIREMENTS

PROCESS

SATISFACTION

HOW?
Change Management Procedure
Including Configuration Management Process

Start With Performance
Process Effectiveness – Change Management Process

Change Management – PEAR Report

Microsoft Office

©2012 ISACA. All Rights Reserved

Follow us @ISACANews
#NACACS
Identity Management Process

Source: Spire Security 2004
Identity Management Functions

- Validate user information
- Create/modify user accounts and privileges
- Disable/delete user accounts
- Change/reset passwords
- Validate sessions
- Authorize access
- Provisioning & deprovisioning

Source: Spire Security 2004
Turtle Diagram – Identity & User Access Management Process

With WHAT?
IT Infrastructure
Site / Facility

With WHO?
CIO, Business Unit Manager

INPUT
Customer Who has a Need

 requirements

PROCESS

HOW?
User Access Management Procedure
Including HR Process

OUTPUT
Customer Who has a Need Met

Start With Performance

©2012 ISACA. All Rights Reserved

Follow us @ISACA News
#NACACS
COBIT & ISO 9001- Alignment with Other Standards

- Both of them harmonize practices and standards such as ITIL, ISO 27001 and 27002, and PMBOK to:
  - Improve their alignment to business needs
  - Cover full spectrum of IT-related activities
1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need to know
8. Assign a unique ID to each person with computer access…
Benefits of Process-based IT Audit

• Process-based (Risk-driven) IT Audit Approach is more effective and value-added than conventional Check-list based approach.

• Use of ISO 9001 based Quality Management System principles can augment the Process-based Audit approach for IT or Information Security.

• Use of Integrated Management System framework based on Quality (ISO 9001), IT Service Management / ITIL (ISO 20000-1) and Information Security (ISO 27001) can be used as the most optimum approach for driving GRC and staying in compliance with minimum cost and efforts.

• Key Performance Metrics (KPIs) and Process Effectiveness Assessment Report (PEAR) are very handy and useful tools to determine effectiveness of a Process in a Process-based IT Audit.
Time for some Exercise......

ARE YOU READY ?..............
Thank You

Questions?
Contact:

ASHIT DALAL, PCI-DSS QSA, CRISC, CGEIT, CISA, CPEA, CSSA SSBB
Certified SCADA Security Architect
Managing Consultant & Vice President – Enterprise Risk Advisory Services
e Delta Consulting, NJ, USA
T.NO: +91-98191-18590 (India)
609-606-2357 (USA)
Email: adalal@edeltaconsulting.com / ashitdalal@yahoo.com
The Knowledge Center is a collection of resources and online communities that connect ISACA members – globally, across industries and by professional focus - under one umbrella. Add or reply to a discussion, post a document or link, connect with other ISACA members, or create a wiki by participating in a community today!