



# IT Audit Process

Michael Romeu-Lugo MBA, CISA

April 24, 2017

# Change Management Project

**Question:** What date range is Q2, and which is Q3? Are the changes in the list without the "Change Request" column filled out with a number "Emergency Changes?"

**Answer:** Our fiscal year starts January 1 and ends 12/31.

- Q1 = Jan 1 – Mar 31
- Q2 = Apr 1 – Jun 30

As for missing change request numbers ("Change Request" column) I don't know. Every change request submitted to our group is issued a number. I would have to get back to you on that.

# Change Management Project

**Question:** Do you have a list of all SysAdmins during Q3? Do you have a list of SysAdmins broken out by responsibility of who creates the changes, who tests the changes, and who migrates the changes to production?

**Answer:** You will find a list of System Administrators in the org chart. Just in case you don't have one you can find it in the attachment.

System Administrators are the only people that can promote changes to production. Once the change has been accepted by the person who requested it the change goes into a queue for System Administrators.

Anyone can create request a change. The change can only be made when it has been approved by the business owner. The change is first made in a development environment. It is only promoted to test when development is complete. UAT is performed in the test environment. The environment in test is a very close approximation of Production. If the Requester is satisfied with the results of the tests he or she approves the change to be promoted to production. At that point is when Sys Admins get involved.

# Reporting Standard 1401 – Reporting

## Statements

**1401.1** - IS audit and assurance professionals shall provide a report to communicate the results upon completion of the engagement including:

- Identification of the enterprise, the intended recipients and any restrictions on content and circulation
- The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed
- The findings, conclusions and recommendations
- Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement
- Signature, date and distribution according to the terms of the audit charter or engagement letter

**1401.2** - IS audit and assurance professionals shall ensure that findings in the audit report are supported by sufficient and appropriate evidence.

# Reporting Standard 1401 – Reporting

Terms	Definition
<b>Relevant</b>	Relating to controls, tells the evaluator something meaningful about the operation of the underlying controls or control component.
<b>Reliable</b>	Information that is <b>accurate, verifiable and from an objective source</b> .
<b>Sufficient</b>	Information is sufficient when evaluators have gathered <b>enough of it to form a reasonable conclusion</b> .
<b>Suitable</b>	<b>Relevant</b> (i.e., fit for its intended purpose), <b>reliable</b> (i.e., accurate, verifiable and from an objective source) and <b>timely</b> (i.e., produced and used in an appropriate time frame) information.
<b>Timely</b>	Produced and used in a time frame that makes it possible to prevent or detect control deficiencies <b>before they become material</b> to an enterprise.

# Reporting Standard 1401 – Reporting: Key Aspects

- **Discuss** draft report contents with management in the subject area before finalize and release. Include management’s response to findings, conclusions and recommendations in the final report.
- It is the responsibility of the Auditor to report significant deficiencies and material weaknesses in the control environment to those charged with governance.
- **Communicate** to audit management internal control deficiencies that are less than significant but more than inconsequential. Notify governance of such communications.

# Reporting Standard 1402 – Follow-Up Activities

## Statements

**1402.1** - IS audit and assurance professionals shall monitor relevant information to conclude whether management has planned or taken appropriate, timely action to address reported audit findings and recommendations.

### Key Aspects:

- The internal IS audit function should establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.
- External IS audit or assurance professionals may rely on an internal IS audit function to follow up on their agreed-on recommendations, depending on the scope and terms of the engagement.

# The Exit Interview



- Purpose
  - Discuss...
    - Findings
    - Recommendations
  - Ensure facts presented in the report are correct
  - Ensure that recommendations are realistic and cost-effective (or look for alternatives)
  - Negotiate implementation dates for agreed recommendations
- Presentation Techniques
  - Executive Summary – communicate from a business perspective
  - Visual Presentation



# The Exit Interview – Things to Consider



# The Exit Interview – Things to Consider



# The Exit Interview – Things to Consider

- Who is the Auditor Responsible To?
  - Audit Committee
  - Senior Management
- Meet with Management Staff regularly during the audit
  - Agree on findings
    - If not, elaborate on the significance of the findings, risks and effects of not correcting the control weakness.
  - Develop a course for Corrective Action
    - Do not become a consultant



# Internal Audit



# Control Self-Assessment (CSA)

- A management technique that assures stakeholders, customers, and other parties that the internal control system of the organization is reliable.

AND

- It also ensures that **employees** are aware of the risks to the business and they conduct periodic, proactive reviews of control.

# Control Self-Assessment (CSA)

## Benefits



- Empower employees to assess or even design control environment
- Early detection of risk
- More effective and improved internal controls
- Employee Engagement
- Sense of Ownership
- Control Cost Reduction

## Disadvantages



- Replace Internal Audit Function?
- Additional Workload
- Damaged employee morale if improvement suggestions not implemented.
- Weak controls may go undetected due to lack of motivation.

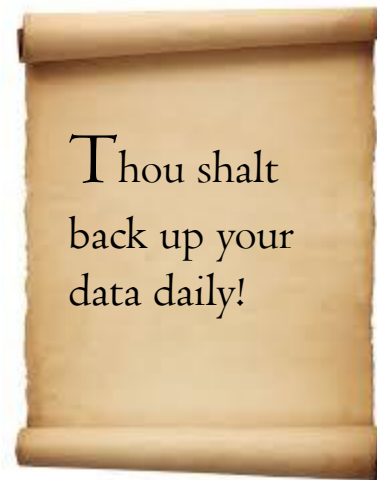
# Control Self-Assessment (CSA)

The CSA approach emphasizes management and accountability over developing and monitoring internal controls of an organization's sensitive and critical business processes.

**NOT Accountability**



# Control Self-Assessment (CSA) The Role of the Auditor





# Control Self-Assessment (CSA) The Role of the Auditor

