Internal Review Methodology

Army Internal Review Review Symposium
Jun-Jul 04
It is better to debate a question without settling it than to settle a question without debating it.

Joseph Joubert
Your Expectations
ANNUAL PLANNING
Condition

There are knowns, known unknowns, and unknown unknowns.

Author unknown
To be prepared is half the victory.

Miguel De Cervantes
Enterprise Risk Management

ERM is a process, effected by an entity’s corporate board, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events, that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

--COSO Fall 2003
In Other Words...

Risk is a concept used to express uncertainty about events and/or their outcomes that could have a material effect on the goals of an organization.

- Paul Walker, Phd., University of Virginia
Risk Management = Misnomer

Risk is not managed, since risk is a conceptual property.

Organizations are managed to anticipate the uncertainty characterized by risk in the environment
Risk Management & Internal Review

- GAGAS: http://www.gao.gov/govaud/ybk01.htm


Internal Review & Risk Management

Auditor’s Risk Management Guide by Paul J. Sobel, CPA, CIA
GAGAS:

1.16 “Audit organizations may also seek to achieve improvement ...’constructive engagement approaches’...for use in responding to current risks, correcting internal control deficiencies...”
GAGAS:

3.15 Auditors may participate on committees or task forces in a purely advisory capacity...Auditors may also provide tools and methodologies, such as best practice guides, benchmarking studies, and internal control assessment methodologies that can be used by management.
IIA: Planning Standard 2010 -

The chief audit executive should establish risk-based plans to determine the priorities of the internal Review activity, consistent with the organization’s goals.
The organization’s risk strategy should be reflected in the internal audit activity’s plan. A coordinated approach should be applied to leverage synergies between the organization’s risk management and internal audit processes.
The internal audit activity evaluates and contributes to the improvement of risk management, control and governance systems.
The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.
IIA: Planning Standard 2120.A1

Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organizations’ governance, operations, and information systems.
Control self-assessment (CSA) methodology can be used by managers and internal auditors for assessing the adequacy of the organization’s risk management and control processes...
Future-Focused Planning Strategy

The Art of the Long View by Peter Schwartz
IR Guide
Chapter 4 - Annual Planning
Risk Oversight – Making sure management has instituted processes to identify and address the major risks the organization faces.

Which of the following risks are included in your internal Review plan?

1. Financial Risks
2. Operational Risks
3. Strategic Risks
4. Other
Annual Internal Review Plan

Start with Organization’s Strategic Plan

1. Identify Review Universe

2. Risk Scenarios
   - Understand Business Process
   - Framework for Discussing Risk with Mgt
   - Process to Open Imagination about Significant Risk Potential

3. Annual Review Plan
Annual Internal Review Plan

IR Guide – Annual Plan Considerations

1. Management Control Program
2. Audit/Oversight Committee
3. Customer Input
Annual Internal Review Plan-
Risk Assessment Tools

<table>
<thead>
<tr>
<th>Performance</th>
<th>Audit Frequency in Months</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Completely Satisfactory</td>
</tr>
<tr>
<td>Risk ($)</td>
<td></td>
</tr>
<tr>
<td>HIGH</td>
<td>12</td>
</tr>
<tr>
<td>MED</td>
<td>16</td>
</tr>
<tr>
<td>LOW</td>
<td>20</td>
</tr>
</tbody>
</table>

Based on single risk factor--$ and results of prior Reviews
TODAY’S BRAIN GAME

26 = L. of the A.

7 = W. of the W.

1001 = A. N.

12 = S. of the Z.

54 = C. in the D. (with the J.)
ENGAGEMENT PLANNING
Risk Management & Internal Review

“Work is to be adequately planned.”

GAGAS: 7.03 – 7.09
When planning the engagement, the internal auditor should identify and assess risks relevant to the activity under review. The engagement objectives should reflect the results of the risk assessment.
IIA: Practice Advisory 2210.A1-1

Internal Auditors should consider the following suggestions when assessing risk during engagement planning....
Risk Considerations

- Activity Objectives and Goals
- Activity Policies, Plans, Procedures
- Organizational Information
- Budget Information
- Prior Reviews/Audits
- Correspondence Files (Congressionals)
- Authoritative/Technical Literature appropriate to activity
REVIEW FIELD WORK
There is nothing so annoying as arguing with a person who knows what they are talking about.

Anonymous
DA IR Guide

Quick Response Reviews: Chapter 6
Consult & Advisory Services: Chapter 7
Liaison: Chapter 8
Follow-Up: Chapter 8
Formal Reviews

IR Guide: Chapter ___
Scheduled on the IR Plan
Quick Response Reviews

IR Guide: Chapter 6

Time Sensitive

1-2 Objectives

Limited Scope

Specific, Selected Fieldwork

Methods

Reduced Workpaper Requirements
Consult/Advisory Services

IR Guide: Chapter 7

Consultation

Verbal or Written Advice: “Comments”

Short Time Frame

Based on Available Information – Limited Research

Advice

Comparison/Analysis of proposed Management Actions

Cost Analysis

Management Control Program Administration
Liaison

IR Guide: Chapter 8

IR – Principal Agent for Command RE: External Audit Agencies

Communication between External Agency & Command

Coordination – Interviews, Site Visits, etc.

Assist Command with Responses/Comments
Follow-Up

IR Guide: Chapter 8

Follow-Up = Integral Part of Review Planning

An audit finding accepted by management = OBVIOUS RISK

Required:

- Formal IR Review Findings
- DODIG & GAO Audits Addressed to the Commander
- AAA Reports subject to the AR 36-2 Reply Process

May Be Necessary for other Audits/Reviews
## Follow-Up

IR Guide: Chapter 8

<table>
<thead>
<tr>
<th>WHAT</th>
<th>WHEN/HOW OFTEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Follow-up Reports</td>
<td>Approval by “command group”</td>
</tr>
<tr>
<td>Status of Open Recommendations* months</td>
<td>As a minimum every 6 months</td>
</tr>
<tr>
<td>■ BY AGE</td>
<td></td>
</tr>
<tr>
<td>Approaching 18 months</td>
<td>e.g., April and October</td>
</tr>
<tr>
<td>[After completion of 1574 Reports]</td>
<td></td>
</tr>
<tr>
<td>REPORTS</td>
<td></td>
</tr>
<tr>
<td>BY SIGNIFICANCE</td>
<td></td>
</tr>
<tr>
<td>Reopened Recommendations*</td>
<td>As required/occurs</td>
</tr>
</tbody>
</table>
Automated Data Gathering

Automated Data Extraction & Analysis

ACL
IDEA
Access
Excel
Others?
Fraud

Automated Fraud Detection and Prevention

ACL
IDEA
DATAS
Others?
IT Security

Network Security Assessment Software
Kane Security Analyst
CyberCop Scanner
Internet Scanner
BindView
NetRecon
Self Assessments

Automated Control/Quality Self Assessments

Internal Self-Developed software
CARDmap
AuditSystem
OptionFinder
The Resolver
Monitoring

Continuous Monitoring Software
Access
ACL
IDEA
SAS
SQL/Internal Developed Software
Documentation

Automated Workpapers
MS Office Suite
TeamMate
AutoAudit
AuditSystem
CARDmap
Some arguments are sound and nothing more.

Richard Armour
Evidence

GAGAS:  7.52 thru 7.61

“Evidence should be sufficient, competent, and relevant to support a sound basis for audit findings, conclusions, and recommendations....”
Review Findings

GAGAS: 7.62 thru 7.65

“...Condition...
...Effect...
...Cause...”
Management: Risk-Based Environment

Proposed COSO Sequence:

1. Establish Organization Objectives
2. Assess Risk
   - Identify It
   - Measure It
   - Prioritize It
3. Manage Risk
   - Control It
   - Avoid It
   - Share It
ENGAGEMENT REPORTS
Review Reports

Format Dependent on Engagement:
Generally--

Objectives

Scope

Methodology

Qualifications RE: Standards

Findings

Recommendations

Management Comments
Review Risk Assessment

Word Substitution – “Risk” vs. “Control”

• Immediate communication links – Mgmt thinks in terms of risk.

• Less friction about Review process—avoids some negative overtones

• Natural flow from Review objective to Review report

• Richer Review planning: Ask Mgmt what risks they worry about
The Review Matrix: An Alternative Report Format?

<table>
<thead>
<tr>
<th>What is the process Now?</th>
<th>What Could Be...The Ideal</th>
<th>So What?..If We Do Nothing</th>
<th>What changes are already Happening?</th>
<th>Recommended Actions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue #1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue #2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue #3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue #4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue #5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
I have discontinued long talks on account of my throat. Several members have threatened to cut it.