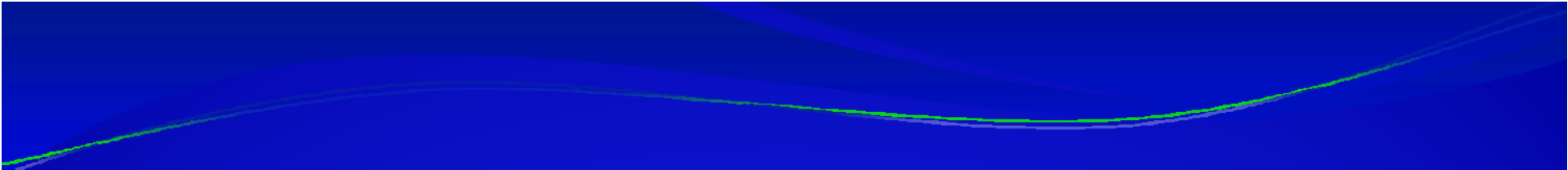


# Risk Based Auditing

Presented by Dr. Catherine L. Martin, DBA  
April 11, 2012



Development of a risk-based quality audit process and support tool to assess risk using a risk-based numerical evaluation system for prioritizing and scheduling audits.

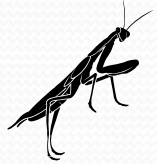
# Quote

Risk-based auditing is probably the most exciting and significant development in the Internal Audit profession's history. It has the potential to catapult the reputation of and the value added by the profession into the stratosphere.

**Griffiths, P. ;Risk-Based Auditing; 2005**

## Risk Based Auditing

What animal best depicts your audit program?



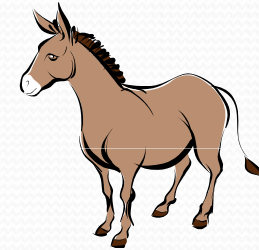
Praying  
Mantis



Bee



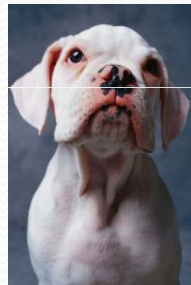
Koala



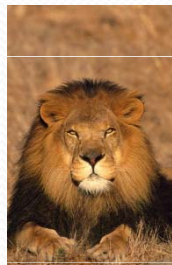
Donkey



Ant



Dog



Lion



Dolphin



Eagle

Griffiths, P. ;Risk-Based Auditing; 2005



# What is Risk-Based Auditing?

Approach

Process



Methodology

Attitude

**Griffiths, P. ;Risk-Based Auditing; 2005**

# What is Risk Based Auditing?

Audit what matters to your organization!

What are the issues that matter?

What are the areas of greatest Risk?

**Griffiths, P. ;Risk-Based Auditing; 2005**



# Why risk based audit planning?

The growing demands for better accountability from all types of organizations in both the public and private sectors has led to great pressures on the internal and external auditors to perform (Pickett, 2006).

# Introduction

Risk management was placed in clause 7.1.2 of the AS9100C Standard to provide additional focus on product risk during product realization. The concept of risk is intertwined within the revised AS9100C standard.



# Introduction

In March 29, 2010 the National Aeronautics and Space Administration (NASA) Quality Program required the implementation of a thorough, disciplined, **risk based approach to quality.**

# Introduction

- Risk based audit approaches represent a major trend in current business and financial audit methodology.
- Developed during the 1990s in response to changes in the business economic communities, the risk based audit represents a new generation of audit approaches.
  - Finance
  - Business
  - Institute of Internal Auditors
  - EHS
  - Canadian Strategic Aerospace and Defense Initiative (SADI)
- Risk based audit approaches are based on risk analysis used to identify business risk commonly defined as a risk that a client cannot achieve its business objectives (Diaz, 2005).



# Finance

- The financial industry has captured considerable attention in recent years, as financial risk management has become a critical corporate activity.
- In the United States, the Sarbanes-Oxley (SOX) legislation enacted by the U.S. Congress in 2002 requires internal controls certifications by the chief executive officers and chief financial officers (Sarbanes-Oxley, 2002).
- **The Institute of Internal Auditors (IIA)** was quick to respond with auditing standards requiring auditors to include risk in audit planning.
  - The IIA's *International Standards for the Profession Practice of Internal Auditing (Standards)* standard 2010.1A requires that the internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually (IIA, 2010).



# Business

- Griffiths (2005) explains the concepts and practice behind a risk-based approach to auditing for business risk management and provides a blueprint for refocusing the internal audit role to embrace risk and to help plan, market, undertake, and report a risk-based audit.
- A detailed audit risk analysis model is predicted on the basis that all risks are relative but that they can be compared by combining three key factors: **(a) the size of the risk or exposure, (b) the controls in place, and (c) the likely effectiveness of the audit.**
- Each of the three factors is given an equal overall weighting, and each topic in the audit is evaluated to **create a score.** The overall scores are combined to create an overall result which can be **ranked** (Griffiths, 2005).

# Canadian SADI

- The Canadian Strategic Aerospace and Defense Initiative (SADI) developed a framework for an integrated Results-based Management and Accountability Framework (RMAF) and Risk Based Audit Framework (RBAF).



# Introduction

- Internal quality audit planning utilizes an audit cycle that ensures each part of the organization is audited for compliance to standards and requirements.
- Internal quality audit plans are typically driven by annual assessments.
- This cyclical approach suggests that the internal quality auditor performs much the same basic audits but in an annual basis.



# Introduction

- With shrinking resources and increased customer pressure, industry professionals must streamline existing processes to reduce costs and resource time needed for compliance management and risk management.
- **New audit tool development is essential to remain competitive while effectively managing risk.**

# Introduction

- The risk based audit support tool's data driven measurement system determines which products and processes get audited.
- Data collected during the study supported the tool's capability to manage risk and reduce costs with no negative impact on current processes, such as AS9100C compliance and audit effectiveness.

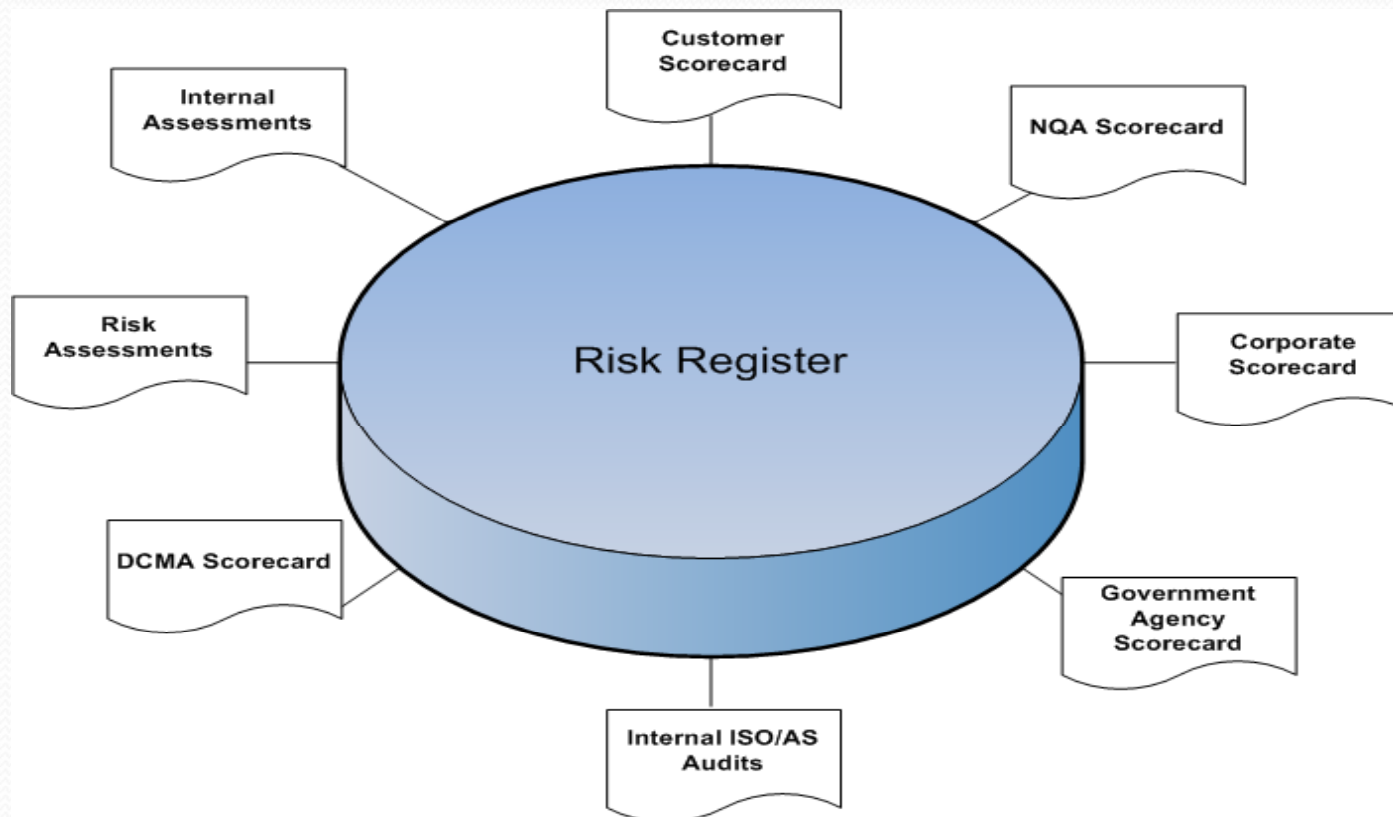


# Introduction

- This study focuses on developing a risk based quality audit process and support tool that describes methods for streamlining the quality audit process and introduces concepts to assess risk and reduce costs using a **risk based numerical evaluation system for scheduling quality audits.**
- Eight existing quality tools are designed to be used together to establish an **overall risk score for audit scheduling.**



# Introduction



**Figure 1. Risk-based audit support tool concept**

# Introduction

- The risk based quality audit process support tool enables more effective use of resources to achieve the same level of effectiveness.
- A support tool key feature is the use of quality data to **drive continual improvement** through identifying areas that are at risk and requesting corrective action via a closed loop corrective action system.



# Introduction

- Resolving problems early in the product life cycle contributes to avoiding costly rework, scrap, and repairs later on.
- The importance of viewing root cause analysis and corrective action as a systematic approach to effectively identify the cause of a nonconformance and to permanently eliminate the source or sources of the problem has been discussed in the literature (Bates, 1998; Hughes, 2000; Paradies, 2010; Royall, 2001).



# Introduction

- Advantage over competitors in that customized internal quality audit process support tool based on risk based planning as an approach to audit work **focuses on strategic, regulatory, and business risks that confront the company, and which uses these risks to steer the audit process in a way that maximizes the impact of the audit on company quality.**
- Audit support tool takes into consideration risk factors directly from commonly available tools.

# Background-Quality Audits

Traditional auditing is a quality management system tool. Used internally, its purpose is to verify that systems are compliant and suitable to achieve objectives. Externally, it may be used to determine compliance to a set of rules.



## Background-ISO/AS Standard

- AS9100C Standard involves implementation of a risk management process throughout product realization (product life-cycle).
  - Risk based auditing provides an opportunity to comply with the new requirement in AS9100C.

# Background-Unit of Measure

- The new risk based audit planning model takes into consideration risk factors derived from an array of tools (i.e. Scorecards).
- Performance Tools currently being used in your company can be converted to a Risk Factor.
- By converting the different scorecard values to a **RPN as a standard unit of measure**, the researcher was able to effectively make comparisons by using a **common reference to the same unit of measurement**.



# Background-Scorecard

- The balanced scorecard is a multi-perspective framework used to develop metrics that claim to support the success of the strategy of an organization (Christesen, 2008).
- Kaplan and Norton (1992) introduced the balanced scorecard as an enhanced performance management system using metrics that go beyond financial results. During the last 10 years, the balanced scorecard has evolved as an extension of the strategy and planning process of an organization (Christesen, 2008).

# Background-Risk

In a dynamic and competitive world, companies cannot manage either strategic or tactical risks by adopting a passive stance. They need to develop the mindset and **tools to explore the many dimensions of risk** associated with each activity and opportunity so that they can balance these against the more obvious signs of reward (Crouhy, 2006).



# Background-Audits & Risk

- The challenge is to develop an audit risk assessment tool that the auditors apply to developing a **relationship between audits and risk management.**
  - Important business processes should be evaluated thoroughly in terms of risk.

# Background-Risk Management

- Risk management does make a difference. Organizations that employ formal risk management practices do outperform those that do not.
- Data collected from 175 web-survey respondents and 12 selective telephone interviewees from the Project Management Institute Risk Management Specific Interest Group answered this question in the affirmative.
- The sample frame represented a wide range of risk management application areas—for example, insurance, financial, operational, environmental, and occupational (Voetsch, 2004).



# Statement of the Problem

- Traditionally audit quality planning utilizes an annual audit cycle that ensures each part of the organization is audited for compliance. This cyclical approach suggests that the internal quality auditor performs much the same basic audits but in an annual basis.
- Important business processes should be evaluated thoroughly in terms of risk by internal quality auditors who directly focus their audit planning in areas that pose unacceptable technical, strategic, and business risk to the company.
- A risk based approach to audit planning simply means that the audit resource is focused on those aspects of the business that are significant to success (Pickett, 2006).

# Purpose of the Study

- This study addressed risk assessment by developing and implementing a risk based internal quality audit process support tool for non-financial institutions.
- The study examined Risk Register as a viable option for use as an audit support tool to ensure audit plans reflects risk to which the company has exposure.



# Hypothesis

“The appropriate combination of Risk Register and performance scorecards into a risk-based audit planning support tool links the risk management strategy to the internal quality auditing strategy which triggers performance improvement efforts.”

# Literature Review

Risk-based auditing was viewed from two points: risk-based auditing in general and risk-based auditing for aerospace and defense. Available industry standards were discussed, as they often drive change.



# Benefit/Contribution

- Management may be able to minimize risk by implementing corrective action and preventive action.
- This may provide a greater return on the organization's investment of people, time, and funding. Further, it may help in improving customer satisfaction and in obtaining new business contracts.
- Ultimately, this study endeavored to help non-financial organizations improve performance through risk-based auditing.

# Methodology

- The study employed mixed methods and consisted of three sequential phases.
  - ❖ Quantitative
  - ❖ Qualitative (Action Research, Case Study)
- The three phases provided data to be used in developing a support tool and quality audit process. Each phase informed the following phase of research activity, thus allowing a degree of triangulation (Creswell, 2003).



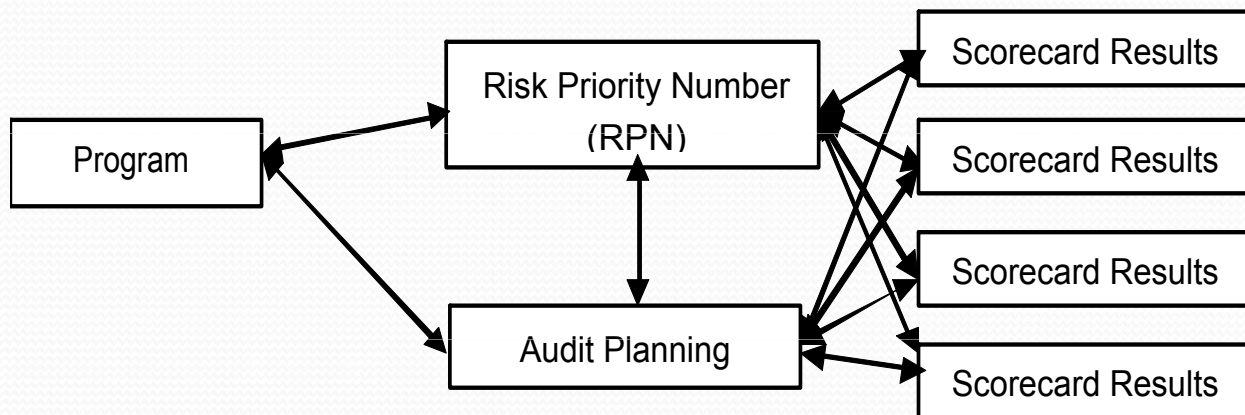
# Methodology-Instrument

- The **Risk Register** is a managed database facilitating consistent application of risk management process criteria such as risk description/risk context, consequence, and risk assessment scales for Cf and Pf; mitigation plans.
- Risk Registers are commonplace in business

# Methodology

Independent Variables

Dependent Variables

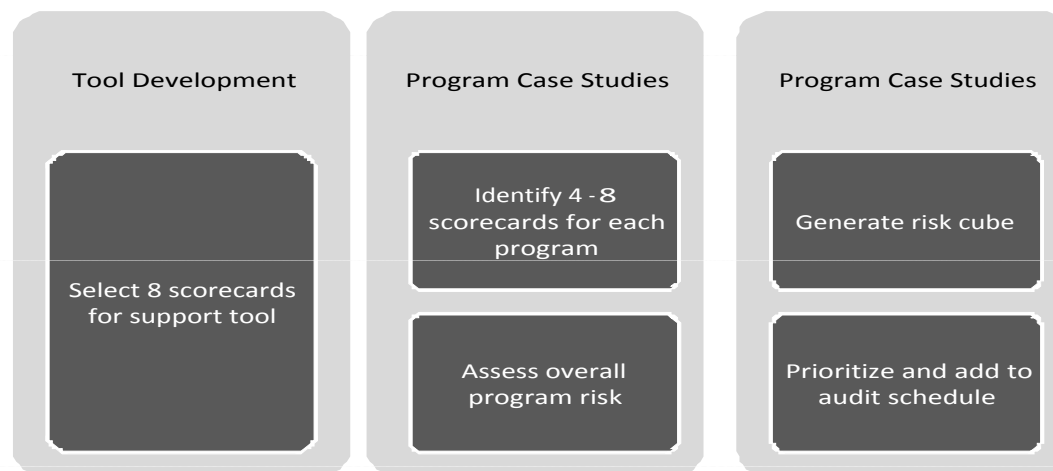


**Figure 2. Research design for analysis of variables**



# Methodology

## Risk Based Audit Process



**Figure 3. Risk-based auditing research study.**

# Methodology -Steps

- Select business areas/processes/programs.
- Select scorecards from an approved list. A minimum of four scorecards per area/process/program is to be analyzed for Risk Priority Number (RPN). Enter the scorecard selection into “RPN Worksheet” form.
- Determine the RPN for each scorecard by using the “Risk Data Collection Sheet” to manually calculate the RPN or by using the Risk Register.

To determine the individual item's RPN enter the scorecard information into Risk Register using the parameters for Probability of Occurrence ( $P_f$ ) and Risk Consequence Factor ( $C_f$ ).

- Scorecard information is converted into a standard unit of measure which is the **RPN value**. The scorecard risk priority numbers for the areas are totaled and averaged.



# Methodology

*Risk Data Collection Sheet for Manual RPN Calculation*

Item	Title	Statement (If, then)	Probability	Consequence	Level ( $R=P \times C$ )	Color rating

**Figure 4. Risk Data Collection Sheet for Manual RPN Calculation**

# Methodology-Example

- Factor ( $R_f$ ) or Risk Priority Number (RPN) was calculated using the following formula:  
Probability ( $P_f$ ) x Consequence ( $C_f$ ).
  - Use your organization's Probability ( $P_f$ ) or Consequence ( $C_f$ ) Scale (i.e. 1-5, 1-10, 0.1 -1.0)
- Risk Level was determined using the following formula:  $R_f$  greater than 0.5 is High,  $R_f$  greater than or equal to 0.25 and less than or equal to 0.5 is Moderate,  $R_f$  less than 0.25 is Low.



# Methodology-Scorecard RPN

- Use the existing color rating of the Scorecard selected and convert to RPN using established risk assessment color ratings.
  - Example: Red Customer Scorecard equates to an RPN of  $> 5$ 
    - $R_f$  greater than 0.5 = High (RED)
    - A risk with  $R_f$  greater than or equal to 0.25 and less than or equal to 0.5 = Moderate (Yellow)
    - A risk with  $R_f$  less than 0.25 = Low (Green)
- If a color rating is not available for the tool, determine individual RPN for each deficiency, nonconformance or finding using Risk Register tool or manual calculation. Average and total to obtain the overall Risk Factor and color rating.

# Methodology-Example Risk Scoring Table

## *Risk Scoring*

Risk factor	Risk level	Status
$Rf \geq 0.5$	High	Red
$Rf \geq 0.25 \leq 0.5$	Moderate	Yellow
$Rf \leq 0.25$	Low	Green

**Figure 6. Risk Scoring table**



# Methodology-Procedure Summary

- Determine overall RPN for each Scorecard selected for each area/process/program.
- Total the RPN for 4-8 selected scorecards for each area/process/program selected.
- Divide by the number of scorecards to obtain an “average RPN”.
- Determine the overall Risk Level (H,M,L).
- Create Risk Cube, rank and map.
- Create Audit Schedule.

# Methodology-Risk Cube

- Use the Risk Cube method for visualizing the risk of each area/process/program.
  - **Prioritize the audit schedule based on the risk levels depicted in the Risk Cube. The ranking of the area/process/programs for risk is graphically displayed in a Risk Cube, a common method of Risk Management.**
- **NOTE: Within each area, you can evaluate the individual scorecards to determine the audit topics.**
- Implement the risk based audit schedule based on a numerical evaluation system for prioritizing and scheduling audits.



# Methodology-Example Risk Cube

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	3	3	4	5
P <sub>f</sub> = Probability or likelihood = 1,2,3,4,5				
C <sub>f</sub> = Consequence = 1,2,3,4,5				
R <sub>f</sub> = P <sub>f</sub> × C <sub>f</sub>				

**Figure 7. Risk Cube**

# Methodology-ANOVA

Analysis of Variance-ANOVA is the most accurate method for quantifying repeatability and reproducibility. In addition, the ANOVA method allows the variability of the interaction between appraisers/Subject Matter Experts and the scorecard items to be determined (Wortman, 2006).



# Methodology

- The Risk Cube can be represented by the Bernoulli Random Variables \*; the expected cost overrun is the sum of cost impacts multiplied by their respective probabilities using the following formula:

- $\text{Cost Risk} = \sum P_f * C_f$

Mean =  $P_f * C_f$

Standard Deviation =  $\text{SQRT} (P_f * (1 - P_f) * C_f) = \text{SQRT} (P_f * Q_f * C_f)$

- \* In probability theory and statistics, the Bernoulli distribution, named after Swiss scientist Jacob Bernoulli, is discrete probability distribution.

# Methodology

- A hypothesis cannot be proven, it can only be supported or refuted, and this is true using either quantitative or qualitative evidence, or both (Seaman, 1999).
- Given the quantitative and qualitative approach used in the current study, the protocol includes assigning risk values to scorecards, ranking of risk for auditing purposes, and implementing a risk-based audit process.



# Methodology

- The three phase approach with a follow-up written review enabled the researcher to validate the scorecard responses with the Risk Register results and ultimately with the performance.
- When empirically-based patterns and trends of data coincide with predicted ones, the case study is believed to achieve internal validity (Yin, 1994).

# Methodology-Limitations

- Caution should be exercised in coming to conclusions and making generalized forecasts to other settings.
- Caution is necessary because most case studies are tailored to a particular group or organization, and any other stakeholders who may be affected by this group or organization (Berg, 2007; Johnson, 2008).



# Results

- This study introduced concepts to assess risk using a risk-based numerical evaluation system for scheduling internal AS9100 audits.
- Existing scorecards were used together to establish overall assignment based on risk. The support tool's data driven risk measurement system determines which area/process/programs get audited and the support tools capability to manage risk and comply with the AS9100C standard.

# Results-Research Questions

- The study developed a **support tool** that would be used to prioritize and schedule audits based on overall risk scores.
- Analyses were performed on data collected from **4-8 scorecards** from five area/process/programs using probability ( $P_f$ ) and consequence ( $C_f$ ) to calculate the **risk level ( $R = P \times C$ )**. The probability scale was 0-1, and the consequence scale 0-1.
- The area/process/program risk metrics are incorporated into a common method of risk management, **the risk cube method**. Upon converting the risk scoring to probabilities and consequences, the list of area/process/programs is **mapped to the risk cube** for analyzing, submitting and communicating results. The information contained in the risk cube is used for risk-based audit scheduling. The risk cube is the optimum tool for applying a relationship between audits and risk management.



# Results-Audit Schedule

Annual audit schedule: All areas can undergo a risk assessment using the risk-based audit support tool for determining overall risk levels and those area/process/programs with high or moderate risk levels are included in the annual schedule.

## Results-Audit Schedule

- The areas were prioritized according to risk levels in the internal audit schedule which enables more effective use of resources to achieve the same level of effectiveness.
- Areas with high and moderate risk levels are audited and resources applied to meet the challenge of addressing the concerns identified in the risk assessment.



## Results-Example

CASE STUDY RISK PRIORITY NUMBER (RPN) WORKSHEET											
Researcher:											
Date:											
	Tool # 1	Tool # 2	Tool # 3	Tool # 4	Tool # 5	Tool # 6	Tool # 7	Tool # 8			
Area/Process/Program	Scorecard or Assessment Tool Description	Scorecard or Assessment Tool Description	Scorecard or Assessment Tool Description	Scorecard or Assessment Tool Description	Scorecard or Assessment Tool Description	Scorecard or Assessment Tool Description	Scorecard or Assessment Tool Description	Scorecard or Assessment Tool Description	Total RPN	Overall RPN	Overall Risk Level
Area A	Internal AS9100 Audit	NQA ISO Recert Scorecard	Customer Scorecard	Risk Assessment	Internal Assessments	Government Scorecard	Corporate Scorecard	Customer Scorecard			
RPN	0.6	0.2	0.3	0.3	0.2	0.25	0.1	0.3	2.25	0.28	Mod
Area B											
Area C											
RPN											

Figure 8. Example Worksheet Results

# Results-Risk Cube Example

Risk Cube										
Probability	10	22	30	40	50	60	70	80	90	100
	0.9	18	27	36	45	54	63	72	81	90
	0.8	16	24	32	40	48	56	64	72	80
	7	14	21	28	35	42	49	56	63	70
	6	12	18	24	30	36	42	48	54	60
	5	10	15	20	25	30	35	40	45	50
	4	8	12	16	20	24	27	32	36	40
	3	6	9	12	15	18	21	24	27	30
	2	4	6	8	10	12	14	16	18	20
	1	2	3	4	5	6	7	8	9	10
Consequence										
P <sub>f</sub> = Probability or likelihood = 0-1										
C <sub>f</sub> = Consequence = 0-1										
R <sub>f</sub> = P <sub>f</sub> XC <sub>f</sub>										

Figure 9. Example Risk Cube Results



# Results-ROI

- One important attribute of most business cases is the development of an economic justification. Return on investment (ROI) is the useful means of gauging the economic merits of adopting and risk-based audit process and support tool.
- Constructing a business case for risk-based auditing does not necessarily require the ROI be greater than zero; that is, that there is a cost benefit. In some cases, the value of the risk-based audit process is not quantifiable in monetary terms.

# Results-ROI

- The aim of using the risk-based audit process and support tool is **cost avoidance**—the reduction or elimination of costs that would otherwise have been incurred—which may be realized in monetary or nonmonetary outcomes.
- Types of **cost avoidance** include failure avoidance, reduced scrap, reduced repairs, reduced risk of catastrophic loss, and increased safety. Cost avoidance may be manifested by improved utilization of a product. In terms of repairs, risk-based auditing may allow for better identification of problems early in the program, decreasing the time needed for inspection and troubleshooting.



# Results-ANOVA

The results of the ANOVA are that the risk appraisers measure the individual risk items in the scorecards in the same way. The results of the ANOVA are shown in Table 5.

# Results of ANOVA

*ANOVA of Risk Appraisers*

Source	<i>DF</i>	<i>SS</i>	<i>MS</i>	<i>F</i>	<i>P</i>
Case	9	0.39417	0.0437969	1.83	0.125
Company	1	0.00110	0.0011025	0.05	0.832
Interaction	9	0.13587	0.0150969	0.63	0.758
Error	20	0.47895	0.0239475		
Total	39	1.01010			

*Note.*  $S = 0.1547$ ;  $R^2 = 52.58\%$ ;  $R^2$  (adj.) = 7.54%.

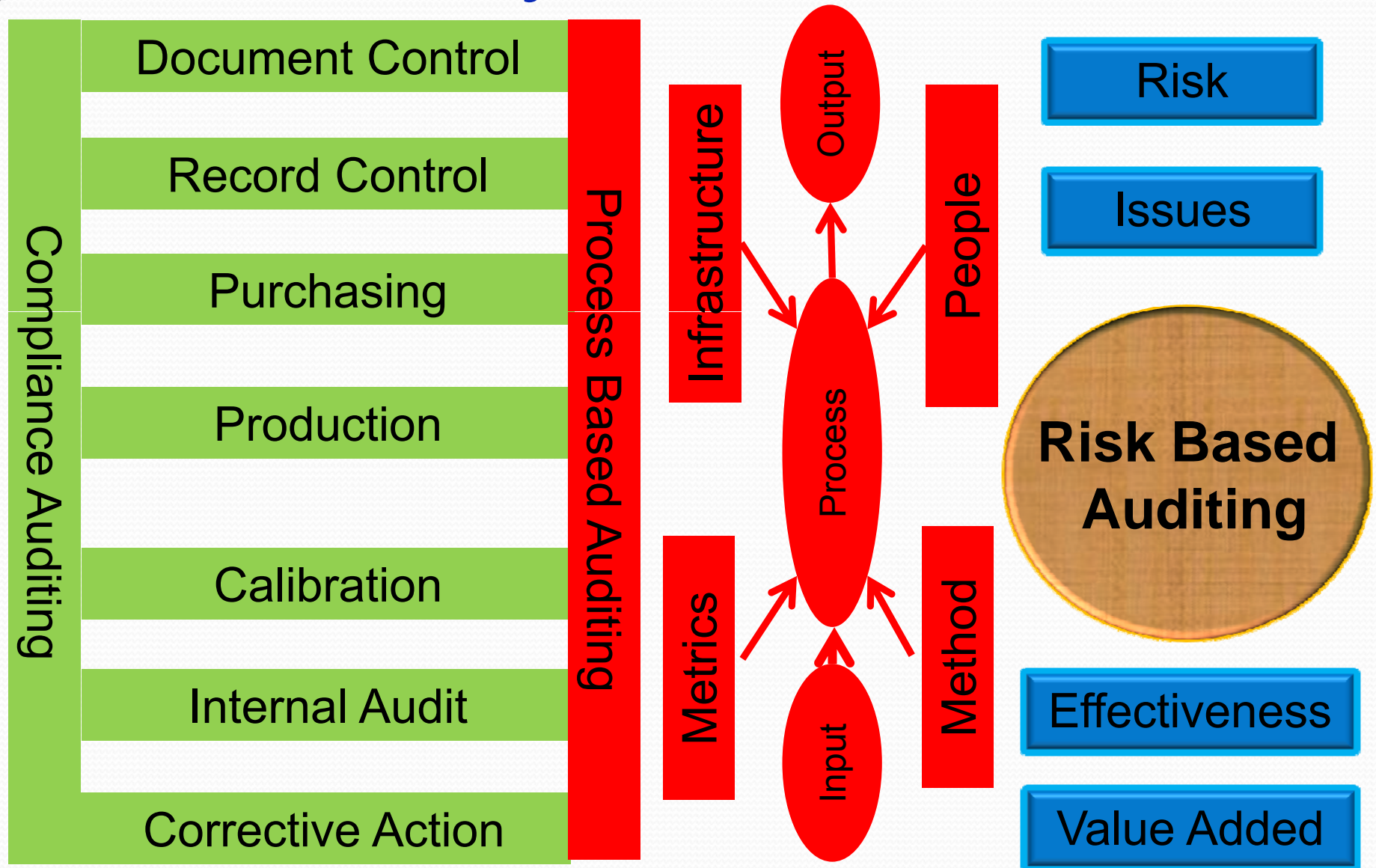
**Figure 10. ANOVA of Risk Appraisers table**



# Results-Summary

- The findings of the area/process/program performance data support the hypothesis and indicate a statistically positive effect for improving performance following an audit as a result of applying the risk-based audit process and support tool for prioritizing and scheduling audits.
- There are three key findings from this research study.
  - First, the researcher found that performance scorecards are tools that can be developed to help auditors respond to changing risk environment.
  - Eight such scorecards were identified in the organization. These tools proved to be well suited to ensuring that auditors had all available risk information for identifying potential risks and developing a risk-based audit.
  - Finally, the researcher found that the common risk management method of “risk cube” to be optimal for building a relationship between audits and risk management.

# History Lesson





# Questions



# Bibliography

AS9100C. (2009, January). *Quality management systems—Requirements for aviation, space and defense organizations*. Warrendale, PA: SAE International.

Bates, T. (1998). The root cause myth. *The TQM Magazine*, 10(1), 10-15.

Berg, B. L. (2009). *Qualitative research methods for the social sciences*. Boston, MA: Allyn & Bacon.

Christesen, D. A. (2008). *The impact of balanced scorecard usage on organization performance*. (Unpublished doctoral dissertation). University of Minnesota- Minneapolis, MN.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative and mixed methods* (2nd ed.). Thousand Oaks, CA: Sage

Crouhy, M. (2006). *The essentials of risk management*. New York, NY: McGraw-Hill.

Diaz, M. C. (2005). *Risk identification and assessment*. (Unpublished doctoral dissertation). College Station, TX.

Griffiths, P. (2005). *Risk-based auditing*. Burlington, VT: Gower.

Hughes, R. L. (2000). *Root cause analysis: Improving the bottom line*. Hopewell, VA: Reliability Center.



# Bibliography

Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard—Measures that drive performance. *Harvard Business Review*, 70(1), 71-79.

Martin, C. L. (2011). *Development of a Risk Based Quality Audit Process and Support Tool For An Aerospace and Defense Company*. National Graduate School-Falmouth, MA.

Paradies, M. (2010, April). Under scrutiny. *Quality Progress*, 32-37.

Pickett, K. S. (2006). *Audit planning: A risk-based approach*. Hoboken, NJ: John Wiley & Sons.

Sarbanes-Oxley Act. (2002). Retrieved from <http://www.soxlaw.com/>

Royall, P. E. (2001). Root cause analysis in a world class manufacturing operation. *Quality*, 40(10), 66-70.

Seaman, C. B. (1999). Qualitative methods in empirical studies. *IEEE Transactions on Software Engineering*, 25(4), 557-572.

Voetsch, R. J. (2004). *The current state of project risk management practices among risk sensitive project management professionals*. (Unpublished doctoral dissertation). George Washington University, Washington, DC.

Wortman, B. (2006). *CQE primer*. W. Terre Haute, IN: Quality Council of Indiana.

Yin, R. K. (1994). Discovering the future of the case study method in evaluation research. *Evaluation Practice* (0886-1633), 15(3), 283.