A Framework for Auditing the Evaluation of Uncertainty for Compliance in Information Systems

Usha Bala Varanasi and B. D. C. N. Prasad

Abstract—**Compliance monitoring in an organization is done by an auditor to ensure that the procedures or mechanisms adhere to the regulatory requirements as intended. An information technology audit assesses an organization's information system and detects potential breakdowns, which are termed as uncertainty. This uncertainty is a quantitative indication of the quality of the result which is expressed in terms of coverage factor. It can moderate the efficiency of an organization. Uncertainty might lead to risk which weakens the business continuity process. In this paper, we propose a framework for evaluating, reducing the uncertainty and associated risks thereby improving the organization's performance and producing realistic and accurate results. This framework provides a base for the empirical evidence stating that 'compliance is affected by uncertainty'. A proper evaluation of uncertainty for compliance is a good professional practice of auditing which provides valuable information about the quality and reliability of the result.**

Index Terms— **Auditing, compliance, evaluating uncertainty, compliance management, IS auditing, mitigation of risks, compliance uncertainty, business continuity.**

I. Compliance Management

Compliance management [1] is an important, costly and complex problem. Compliance management provides a common framework and an integrated approach to manage all compliance requirements faced by an organization to manage cross-industry regulations and policies.

Managing compliance is a very *expensive* endeavor. The compliance management reduces the compliance costs by enabling consistent compliance and control, eliminating deviations and errors, and automating information inflows. Compliance management system is a program designed to ensure that the policies and practices that are implemented in the organization are in full compliance of federal policies and laws. Structured compliance management system establishes compliance responsibilities. It then communicates these responsibilities to employees. It paves a way to incorporate policies into practice. It also establishes accountability for meeting requirements through policies, practices and corrective measures. Compliance can be attained by mitigating risks and uncertainties in the organization.

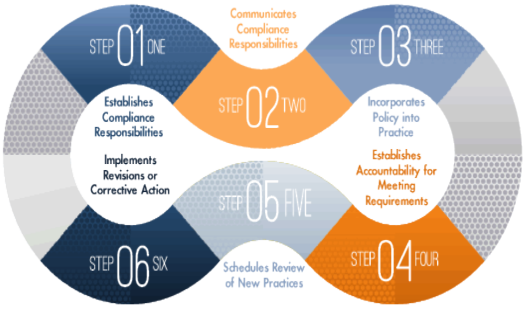
STEP 01 ONE
Communicates Compliance Responsibilities
STEP 03 THREE
Establishes Compliance Responsibilities
STEP 02 TWO
Incorporates Policy into Practice
Implements Revisions or Corrective Action
STEP 05 FIVE
Establishes Accountability for Meeting Requirements
STEP 06 SIX
Schedules Review of New Practices
STEP 04 FOUR

Fig. 1. Compliance management system.

II. Information System Audit

An audit is a planned and documented activity performed by qualified personnel to determine by investigation, examination, or evaluation of objective evidence, the adequacy and compliance with established procedures, or applicable documents, and the effectiveness of implementation [2]. The purpose is to evaluate and improve the effectiveness of risk management, control and governance processes.

Regulatory compliance audits are used to evaluate and measure how well a company is adhering to mandatory regulations. Many professionals rely on compliance techniques such as technical assessments, self-assessment questionnaires, risk assessments and numerous observation techniques in change management which may lead to gaps in the organization when failed to do so. This increases the importance of continuous auditing and continuous controls monitoring approaches. Organizations should work to comply on managing configuration controls on systems and applications, managing system and application security, and managing business continuity and plans.

Information Systems (IS) audit is an examination of the management controls within an information technology infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding the assets, maintaining the data integrity, and operating in a systematic manner to achieve the organization's goals or objectives. IS audit improves an organization's efficiency and profitability by better understanding about their working and financial systems, identifying the areas that need improvement by facilitating change management. The most important aspect of IS audit is that it can uncover uncertainties and inaccuracies within an organization by providing accurate final result.

III. Uncertainty

Uncertainty is a set of consequences where the

Manuscript received February 12, 2014; revised April 18, 2014.

Usha Bala Varanasi is with Anil Neerukonda Institute of Technology and Sciences, Department of IT&MCA, Sangivalasa, Visakhapatnam,Andhra Pradesh, India (e-mail: kasibhattaushabala3@gmail.com).

B. D. C. N. Prasad is with Department of MCA,PVP Siddhartha Institute of Technology, Kanuru, Vijayawada, Andhra Pradesh, India (e-mail: bdcnprasad@gmail.com).

DOI: 10.7763/LNSE.2015.V3.162

probabilities of these outcomes are completely unknown. A state of having limited knowledge where it is impossible to exactly describe the existing state, a future outcome, or more than one possible outcome is said to be uncertainty. A parameter, associated with the result of a measurement that characterizes the dispersion of the values that could reasonable be attributed to the measurand [3].

It is a parameter associated with the result of a measurement (calibration) that defines the range of values that could be attributed to the measured quantity (measurand). The uncertainty is a quantitative indication of the quality of the result [4]. It allows the assessment of the reliability, by comparing the results from various sources or with reference values which can be evaluated by combining a number of uncertainty components that are quantified either by evaluation of results or repeated measurements or by estimation based on data from previous records, measurements and experience.

Measurement of uncertainty indicates compliance or non-compliance with a specification. To assess compliance with an upper specification limit, fig.2 shows the expanded uncertainty ±U on each result and the associated curve indicates the inferred probability density function for the value of the measurand, showing that there is a larger probability of the value of the measurand lying near the centre of the expanded uncertainty interval than the ends.

Batch 1) clearly states that the measurement results and their uncertainties provide good evidence that the value of the measurand is well above the limit. Batch 2) there is high probability that the value of the measurand is above the limit but the limit is within the expanded uncertainty interval. Batch 3) states that the probability that the value of the measurand is below the limit and may not be sufficient to take the result to justify the compliance. Batch 4) states that the measurement results and their uncertainties provide good evidence that the value of the measurand is well below the limit.

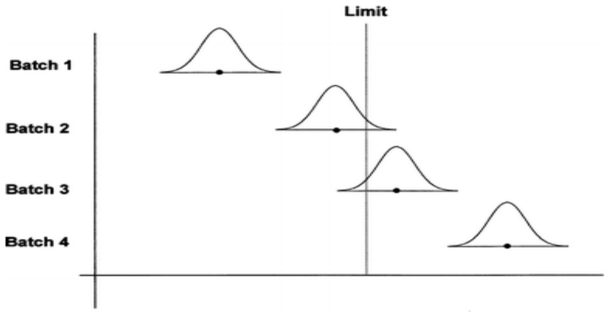

Fig. 2. Assessment of compliance with an upper limit.

IV. Uncertainty Assessment

The need for an adequate assessment has been highly emphasized to achieve the significance of strong controls through compliance assessment. A key component in achieving this is to adopt a good compliance assessment technique or a framework.

The benefits of compliance assessment include: best practices of content database, advanced collaboration of tools: to create, review, approve, update and evaluate responses, capabilities for implementing compliance processes in a timely manner and to gain in-depth knowledge for better decision making. This can be acquired by the evaluating the expanded uncertainty by coverage factor, decision rules and acceptance zones.

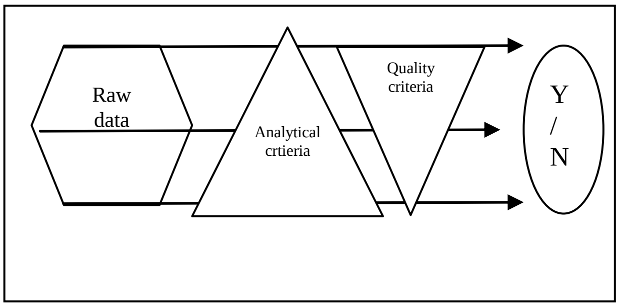

Fig. 3. Assessment of compliance.

V. Solutions for Uncertainty

A. Expanded Uncertainty

Expanded uncertainty represents an interval that contains true value on the required confidence level and it is defined in the document [5]. The additional measure of uncertainty that contains a large fraction of expected values of the measurand is called expanded uncertainty and is denoted by the symbol *U*, and is calculated as, the combined uncertainty multiplied by coverage factor,

$$U = k.\, u\, c\,(\, y\,)$$

where *U* is the expanded uncertainty, *k* is coverage factor and $u\, c\,(\, y\,)$ is standard combined uncertainty. The compliance is evaluated by measuring this uncertainty which is directly proportional to the value of the measurand.

The main role of coverage factor is to expand the interval that belongs to the combined uncertainty so that final interval will contain true value with the required confidence level.

B. Decision Rules and Acceptance Zones

The compliance assessment can be acquired by “decision rules and acceptance zones”. The “Acceptance zone” and the “Rejection zone” are based on the decision rules. These are the rules that are used for the acceptance or rejection of a product based on the measurement result i.e. its uncertainty and the specification limits, taking into account the acceptable level of the probability making a wrong decision. If the measurement result lies in the acceptance zone, the product is declared as compliant and if it is in the rejection zone, it is declared as non-compliant. This result implies the non-compliance with an upper limit if the measured value exceeds the limit by the expanded uncertainty. In the above Fig. 2; batch 1) would imply non-compliance. If a result is equal to or above the upper limit implies non-compliance: batch 3) and batch 4) implies non-compliance, and a result below the limit implies compliance i.e. batch 2), provided that uncertainty is below a specified value.

The requirements for determining whether to accept or reject the calibration test items are:

- A specification: giving upper and lower limits of the characteristics.
- A decision rule: that describes how the measurement uncertainty will be taken into account with respect to

acceptance or rejection zones.

- The limits of the acceptance and rejection zones: derived from decision rules should be within the appropriate zone.

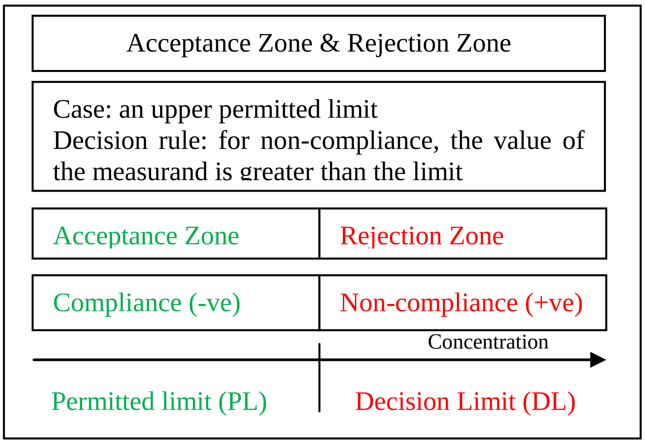
Acceptance Zone & Rejection Zone
Case: an upper permitted limit
Decision rule: for non-compliance, the value of the measurand is greater than the limit
Acceptance Zone
Rejection Zone
Compliance (-ve)
Non-compliance (+ve)
Concentration
Permitted limit (PL)
Decision Limit (DL)

Fig. 4. Acceptance and rejection zones.

VI. Risk

Risk can be defined as imperfect knowledge where the each action leads to a set of possible outcomes each with a known probability. Risk also can be stated as uncertain consequences and has three components: the event that could occur, the probability that the event will occur, and the impact that the event would have on the project should that event occur [6]. A risky situation is a situation where the outcome is unknown to the decision-maker and is not sure which outcome will occur and the uncertainty may lead to erroneous choices.

Risk is a natural part of the business landscape. If left unmanaged, the uncertainty can spread like weeds, if managed effectively, losses can be avoided and benefits obtained [7]. This implies risk management is essential for business continuity. A risk management process provides a strategic orientation for organizations of all sizes in all geographical areas with a formal process to identify measure and manage risk.

VII. Risk Management

Effectively managing the business risks is essential to an organization's success. The process of identification, analysis and either acceptance or mitigation of uncertainty in investment decision-making is known as risk management. Risk management is a step by step process that constitutes: identifying the risks, assessment of risks, determining what risks exist and then handling those risks in a way best-suited. Risk management can be defined as choosing among the alternatives. Risk mitigation and planning efforts may necessitate that organizations set policies, procedures, goals and responsibility standards. This results in better cost management of the organization.

Risk management tools and techniques include brainstorming, event inventories and loss event data, interviews and self-assessment, facilitated workshops, SWOT analysis, risk questionnaires and risk surveys.

Risk-based compliance enables resources to be targeted to the areas where they are most needed and will prove most effective. This has numerous benefits for the organization that incorporates improved compliance outcomes, efficiency gains, reduced business compliancy costs and provides support for compliance measures.

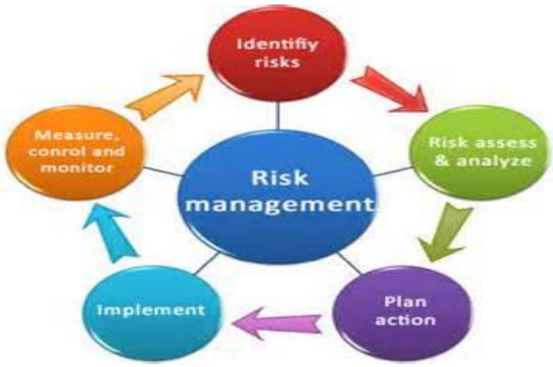

Fig. 5. Risk management.

VIII. Proposed Framework

Uncertainty can moderate the planning and performance effects of the organization. Uncertainty is inversely proportional to the organization's performance. The lower the uncertainty the higher is the performance of the organization. The higher the uncertainty the lower is the performance of the organization. The problem of uncertainty can lead to risk which are to be mitigated for desired outcomes. Risk and uncertainty, both depend on "who knows what" strategy.

The proposed framework helps to overcome both the risk and uncertainty and helps to attain accurate results. It encompasses that risks and uncertainty are managed appropriately and consistently to comply with information systems audit. It also facilitates the sharing of approaches and helps in taking appropriate and corrective action necessary to manage compliance.

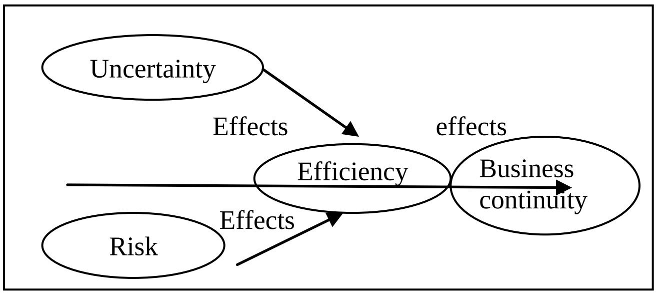

Fig. 6. Effects of uncertainty and risk on business continuity.

IX. Future Work

This approach of evaluating the uncertainty for compliance can be combined with various compliance strategies of information systems thru the implementation of frameworks, which helps in regulatory compliance. This approach can also be implemented with other risk assessment tools like COBIT, SIX-SIGMA etc. in attaining confidential and desired results. Complying with regulations and policies remains as a challenge.

Compliance means conforming to a rule, specification or a policy. Regulatory compliance is the goal of achieving the efforts in order to comply with organization's relevant laws and regulations. As business processes become technologically sensitive, the areas of technology governance and compliance will remain highly significant for the future.

X. Conclusion

Uncertainty is an avoidable part of any measurement and it starts to matter when results are close to a specified limit. Proper evaluation of uncertainty is a professional practice that provides accurate and reliable results. This helps in reducing the uncertainty thereby providing compliance to the information systems. Mitigation of risks in order to achieve the desired outcome through reliability, robustness, interoperability, versatility, which form the basics of information system. The proposed framework reduces the uncertainty and helps in complying with the standards and policies of the organization at a minimum cost. It also ascertains that the accurate outcomes are achieved to promote business continuity.

Acknowledgments

I would like to thank IACSIT Advisory Committee and calibration assessors for their efforts in reviewing the manuscript and providing recommendations.

In particular, I gratefully acknowledge Dr.B.D.C.N.Prasad, Dr. Sumit Gupta, Dr. V. S. R. K. Prasad, Mr. Venkat Sanapala for their wise and valuable suggestions.

Finally, this guidance could not have been written without the support and encouragement of my family, advisory committees and management.

References

[1] A. Tarantino, *Governance, risk and Compliance handbook*, New York: Wiley, 2008.

[2] D. H. Stamatis, *Audit defined in Six Sigma and Beyond: The Implementation Process Volume VII*, CRC Press, 2002.

[3] *ISO/IEC Guide 99:2007, 2.3-Uncertainty of Measurement, ISO Guide*, The Open Toxicology Journal, vol. 6, Suppl 1, 2013, pp. 20-26.

[4] G. H. White and I. Farrance, "Uncertainty of Measurement in Quantitative Medical Testing," *Clin Biochem Rev.*, A Laboratory Implementation Guide, vol. 25, no. 4, Nov. 2004, pp. S1-S24.

[5] ISO 21748:2010 – 2.2--2.3.5-Expanded Uncertainty, *Guide to the Expression of Uncertainty in Measurement*.

[6] P. Otomański, "Calculation of the approximate coverage factor value for the convolution of two Student's distributions and one rectangular distribution," *Measurement Science Review*, vol. 5, Sect. 1, 2005.

[7] T. James, *Managing Information Technology Projects: Applying Project Management Strategies to Software, Hardware, and Integration Initiatives*, AMACOM, 2004.

Usha Bala Varanasi is an assistant professor in Anil Neerukonda Institute of Technology and Sciences, Sangivalasa, Visakhapatnam, Andhra Pradesh since June 2012. She has done her masters in computer networks and information security. She is pursuing her doctoral studies in the area of information security auditing, computer science. She is a member of professional societies such as IACSIT, IEEE, IACQER and ACM. She published papers in reputed journals and international conferences. Her areas of interest include compliance management, information systems, regulatory compliance, and information security auditing, compliance frameworks.

B. D. C. N. Prasad is currently working as a professor and the head, Department of Master of Computer Applications, Prasad. V. Potluri Siddhartha Institute of Technology, Kanuru, and Vijayawada-7. He has an excellent academic and research experience. He has contributed various research papers, in the national and international conferences and journals. He is a member of professional societies such as IEEE, ACM, ISTAM, ISTE, IACQER and APSMS. His areas of interest include applied mathematics, microwave engineering, computer networks, network security and applications, artificial intelligence and applications, game theory, information technology and computer networks.