www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-2, April 2018
Review Paper

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

# Significance of ISO/IEC 27001 in the Implementation of Governance, Risk and Compliance

**Sanskriti Choubey[1]*, Astitwa Bhargava[2]**

[1*] Master of Science in Cyber Law and Information Security, National Law Institute University, Bhopal, India.
[2] Rajeev Gandhi National Cyber Law Centre, National Law Institute University, Bhopal, India.

Received: 11/Mar/2018, Revised: 20/Mar/2018, Accepted: 19/Apr/2018, Published: 30/Apr/2018

***Abstract-***In organisations, ‘Governance’, ‘Risk’ and ‘Compliance’ (GRC) are among the basic and strongest pillars that work together for the purpose of assuring organizations in meeting their objectives through effective utilization of the available people, process and technology. It is challenging task for most enterprises for sustaining Information Security GRC program with the evolving governance needs, changing risk environment and multiple compliance requirements. ISO 27001:2013 encompasses all the goals of GRC under its Information Security Management System (ISMS) framework through which an effective GRC framework could be established and maintained. In this research paper, researcher have established the relationship between ISO 27001:2013 and GRC while discussing the standard along with GRC objectives.

***Keywords***: *ISO/IEC 27001:2013, GRC, ISMS, Risk Management, IT Governance.*

## I. INTRODUCTION

In the early days of GRC, PricewaterhouseCoopers[3] observed: “In itself GRC is not new. As individual issues, governance, risk management[4] and compliance have always been fundamental concerns of business and its leaders. What is new is an emerging perception of GRC as an integrated set of concepts that, when applied holistically within an organisation, can add significant value and provide competitive advantage.”[5]

ISO/IEC 27001:2013 (ISO 27001) is the international standard that provides best practice for an ISMS (information security management system). Achieving certification to ISO 27001 demonstrates that an organisation is following information security best practice, and provides an independent, expert verification that information security is managed in line with international best practice and business objectives.[6]

An integrated approach to GRC with ISMS strategies and controls would be explained in the paper. Firstly a brief introduction to ISO 27001:2013 would be given then GRC would be discussed along with comparision of goals of both then some issues and their countermeasures would be discussed.

## II. ISO 27001:2013

The series of information security standards is also known as the ISO 27000 series, is developed and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)[7] to provide a globally recognised and accepted framework for best-practice in Information Security Management.

[3] PricewaterhouseCoopers is a multinational professional services network headquartered in London, United Kingdom. It is the second largest professional services firm in the world, and is one of the Big Four auditors, along with Deloitte, EY and KPMG from *https://en.wikipedia.org/wiki/PricewaterhouseCoopers.*

[4] Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact from *https://en.wikipedia.org/wiki/Risk_management.*

[5] Accessed from https://mafiadoc.com/a-frame-of-reference-for-research-of-integrated-citeseerx_599dff481723dd0b40ac6283.html.

[6] Accessed from https://www.itgovernance.co.uk/iso27001.

[7] The International Electrotechnical Commission is an international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as "electrotechnology" from https://en.wikipedia.org/wiki/International_Electrotechnical_Commission.

ISO/IEC 27001:2013 is the best-known standard in this family of standards which imparts with the requirements for an Information Security Management System (ISMS). The standards in the ISO/IEC 27000 family helps organizations in keep information assets intact by managing the security of assets such as financial information, intellectual property, employee details, business secrets or third parties information.

An ISMS is a systematic approach of managing sensitive company information. It includes people, processes and IT systems by applying a risk management process and can be implemented in any kind of industry. Like other ISO management system standards, certification to ISO/IEC 27001 is possible but not mandatory. Some organizations choose to implement the standard in order to gain benefits from the best practice while others decide they also want to get certified to reassure its customers and clients that its recommendations have been followed. ISO does not perform certification, certification agencies do.

## III. GRC (Governance, Risk and Compliance)

### 3.1Governance

Governance defines management approach where senior executives direct and control the entire organization, collaborating management information and hierarchical management control structures.

### 3.2Risk

In Risk Management a set of activities are performed through which management identifies, analyses, and treats where necessary, by responding appropriately to risks that might adversely affect in meeting organization's business objectives.

### 3.3Compliance

Compliance with specified requirements, is achieved through management processes which identify requirements, assess the state of compliance, risks & potential costs of non-compliance against projected expenses to achieve conformance.

The purpose of GRC is to provide an overall 360-degree view of risk and compliance, and to identify inter-relationships in today’s complex and distributed business environment and manage them.

GRC is a federation of business roles and processes, working together as a common framework, collaborating and designing to achieve agility, effectiveness, and efficiency across the entire organization.

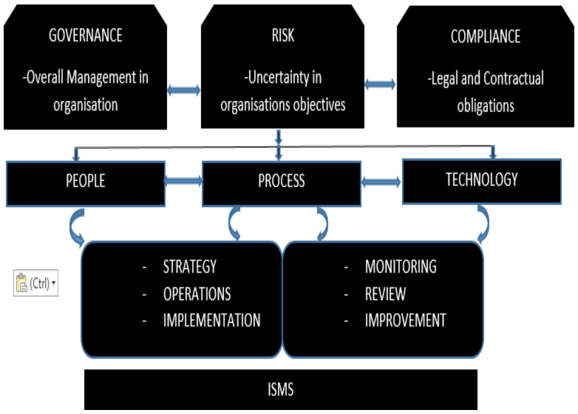
## IV. Mapping goals of GRC with ISO 27001:2013 standard clauses:

The goals of GRC can be mapped with the clause of the ISO 27001:2013 standard for finding the similarities between them.

<table>
<tr><th>S.NO</th><th>GOALS OF GRC</th><th>CLAUSE NO.(ISO 27001)</th><th>ISO 27001:2013 CLAUSE</th></tr>
<tr><td><b>1.</b></td><td>Understanding and prioritizing stakeholders expectations</td><td><b>4.2</b></td><td>Understanding the needs and expectations of interested parties</td></tr>
<tr><td colspan="4"><i>Explanation-The stakeholders/interested parties needs and expectations are gathered in detail to fulfil their requirements and ensure the results are as per their desire.</i></td></tr>
<tr><td><b>2.</b></td><td>Setting business objectives that are congruent with the risk and values</td><td><b>6.1</b></td><td>Actions to address risks and opportunities</td></tr>
<tr><td colspan="4"><i>Explanation-The risks and the opportunities associated with the organisation must be aligned with the Business objectives.</i></td></tr>
<tr><td><b>3.</b></td><td>Achieve objectives while optimizing risk profile and protecting value</td><td><b>8.1</b></td><td>Operational planning and control</td></tr>
<tr><td colspan="4"><i>Explanation-Planning, implementing and controlling the processes needed to meet discipline-specific requirements, including the actions to address risks and opportunities.</i></td></tr>
<tr><td><b>4.</b></td><td>Enable Measurement of performance</td><td><b>9.1</b></td><td>Monitoring, measurement, analysis</td></tr>
</table>

| | | | |
|---|---|---|---|
| | and its effectiveness | | and evaluation |
| *Explanation-Performance evaluation must be done for finding out the scope of improvement.* | | | |
| **5.** | Providing reliable and timely information to the stakeholders | **9.3** | Management review, feedback from stakeholders |
| *Explanation-A transparent reliable system must be maintained in the organisation while keeping stakeholders associated with their respective projects.* | | | |
| **6.** | Operating within legal, contractual, internal, social and ethical boundaries. | **A.18.1** | Compliance with legal and contractual requirements |
| *Explanation-The associated Legal, contractual and social obligations must be kept in mind while implementing any management system in the organisation.* | | | |

## V. FIGURE – ISMS INTEGRATION WITH GRC.



## VI. ISSUES

Issues associated with integration of ISMS with GRC includes, alignment of operational security with Risk Management, Business Continuity and other compliance programs also, organisational alignment of risk and compliance metrics and controls across functional domains and also management of regulatory complexity to reduce the cost of compliance.

## VII. COUNTERMEASURE

*A.* Different automated tools are being used in organisations to counter the discovered issues and challenges faced in the integration of ISMS with GRC. SecureAware IT GRC Management System8, SAP-GRC9, iServer Business & IT Transformation Product Suite [ORBUS][10] and GRCPerfect - Enterprise Portfolio, Project Governance, Risk and Compliance Management System are some of the automated systems which are being used in various companies.

Illustration of GRCPerfect -

GRCPerfect - Enterprise Portfolio, Project Governance, Risk and Compliance Management System

[8] This is the product overview for the IT GRC solution: SecureAware IT GRC Management System. And its five modules: Policy TNG, Risk TNG, Awareness, Compliance and BCP from https://list.ly/list/GjU-grc-tools-to-manage-your-isms.

[9] SAP BusinessObjects Governance, Risk and Compliance (GRC) solutions offer organizations with solutions that address risk management, corporate governance and regulatory compliance from https://list.ly/list/GjU-grc-tools-to-manage-your-isms.

[10] Explore the iServer Business & IT Transformation Suite, a range of tools for Enterprise Architecture (EA), Business Process Analysis (BPA), Governance, Risk & Compliance (GRC) and more from https://list.ly/list/GjU-grc-tools-to-manage-your-isms.

GRCPerfect is an Enterprise Governance, Risk, and Compliance Management System. It is designed to help companies implement IT Governance11, Quality, and Information Security Management Systems in an integrated manner. It has some characteristics like, extremely user-friendly, simple and easy to maintain yet very cost effective. It has pre-built automated processes for CMMI 512, ISO 27001, ISO 20000[13] and ISO 9001[14.] It is a complete data management system for CMMI, ISO 9001, and ISO 27001 standards.

GRCPerfect is based on the industry best practices and bench marked against international standards/models/best practices such as Balanced Scorecard, CMMI, ISO 9001, and ISO 27001.

Key benefits of deploying GRCPerfect

- Minimum 50% effort reduction in deploying GRC frameworks in the organization
- Unified tool to implement best practices from multiple-world class frameworks such as ISO (9001, 27001, 20000, 14000, 18000), CMMI, ITIL[15], Business.
- Senior Management and client visibility into Organizational, Account and Project level performance parameters
- Improved data and metrics integrity, thus helping in better decision making
- Significant help in ongoing process sustenance beyond audit and assessment
- Complete automation of project management artifacts and reporting – significant savings on management effort.[16]

## VIII. CONCLUSION

GRC aligns business processes, partners, employees, and systems to be more efficient and manageable. Non-conformities, errors, and potential risks can be identified, averted, or contained, reducing exposure of the organization, and ultimately creating better business performance.

Organisations follow a proactive approach in tracking and analysing risks with its GRC platform, risk intelligence, and efficient service modules, helping for enhancement of operational, regulatory and business risk management. An integrated GRC with ISMS approach avoids overlapping and duplication of risk management activities and processes with sustainable cost-effective methods.

## ACKNOWLEDGMENT

I would like to express my sincere thanks of gratitude to the faculties at NLIU, Bhopal who gave me the guidance to do this work of research.

## REFERENCES

[1] Ernest N Young Company “Implementing-a-governance-risk-and-compliance-program “
[2] Risk & Compliance (GRC) Institute for Software Technology and Interactive Systems “A Frame of Reference for Research of Integrated Governance”.
[3] EMC Corporation “The case for GRC –addressing the top 10 GRC challenges”- white paper.

[11] *IT governance* is a framework that ensures your organisation's IT infrastructure supports and enables the achievement of its corporate strategies and objectives from *https://www.itgovernance.co.uk/it_governance.*

[12] CMMI can be used to guide process improvement across a project, division, or an entire organization. CMMI defines the following maturity levels for processes: Initial, Managed, Defined, Quantitatively Managed, and Optimizing from https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration.

[13] ISO 20000 is a global standard that describes the requirements for an information technology service management (ITSM) system from searchcio.techtarget.com/definition/ISO-20000.

[14] *ISO 9001*:2015 sets out the criteria for a quality management system and is the only standard in the family that can be certified to from https://www.iso.org/iso-9001-quality-management.html.

[15] The ITIL (Information Technology Infrastructure Library) has become the de facto standard in IT Service Management. ITIL helps organizations across industries offer their services in a quality-driven and economical way. The framework’s most recent version, published in 2011, is only a progressive update that further refines an existing body of IT Service best practices from https://www.simplilearn.com/itil-key-concepts-and-summary-article.

[16] Accessed from http://adaptiveprocesses.com/grcperfect.html.