



# Holistic Approach to Cloud Security - The Governance, Risk Management & Compliance Way

Authors  
Malini Rao & Varun Kashyap

# Contents

- Introduction
  - Why GRC Assessment
- Benefits of Cloud computing and Problem Statement
  - Key Speculations & Problems faced by Cloud service user's in Today's time
    - Threats, Vulnerabilities and related Risks
- Wipro Recommendation: GRC Framework for Cloud Computing
  - GRC Framework
  - Identified GRC Domains
  - Assessment Tools- Solution.
- Wipro Recommendation: Top 4 Action Points to Strengthen Cloud Computing Security.
- Conclusion
- Acronyms
- References
- About the Authors
- About Wipro Consulting Services

## Introduction

“Do more with less” is key objective for CXO for current financial year. The IT industry has been waiting for the next big thing and two words that rock the world is “Cloud Computing”. Because Cloud computing promised the means to achieve the objective. All though a lot of speculation has been going around with respect to security, privacy, governance, compliance, etc related issues within Cloud computing.

As per the latest report by Gartner on ‘Top End user Predictions 2010’. Key predictions summarized below are related to more and more use of Web access and cloud computing services in future leading to increased threats, vulnerabilities and risks to cloud computing security.

- By 2012, 20% of businesses will own no IT assets.
- By 2012, India-centric IT service companies will represent 20% of the leading cloud aggregators in the market.
- By 2012, Face book will become the hub for social networks integration and Web socialization.
- By 2014, most IT business cases will include carbon remediation costs.
- In 2012, 60% of a new PC's total life greenhouse gas emissions will have occurred before the user first turns the machine on.
- Internet marketing will be regulated by 2015, controlling more than \$250 billion in Internet marketing spending worldwide.
- By 2014, more than three billion of the world's adult population will be able to transact electronically via mobile and Internet technology.
- By 2015, context will be as influential to mobile consumer services and relationships as search engines are to the Web.
- By 2013, mobile phones will overtake PCs as the most common Web access device worldwide.

In recent past there have been many cases where a customer/client has faced major problems in accessing their own data due to server crash down or legal action against a cloud provider. Google faced a server outage for its mail service which led to a downtime of more than 100 minutes during which many Gmail users were unable to access their emails. A similar problem but in a different format was faced by Pirate Bay customers, when their systems were seized by the police they couldn't find their own websites /or data storage in place. Many of them who were not even involved with The Pirate Bay, lost their servers and systems and still have not gotten them back near two years later.

Another area where Cloud Computing is facing hurdles is privacy and security the basic data or business information which is housed on a Cloud Service providers Server. There has been speculation's that although there is a cost benefit to outsource the entire IT Infrastructure and focus on one's own Core Competencies, but due to number of incidences the reliability to use it has still not come in majority of the IT Sector all over the globe. Wipro has come up with a Governance, Risk and Compliance (GRC) approach for Cloud Computing in order to tackle these issues and provide a unified solution for Cloud Service providers as well as its Customers.

It can be clearly seen that although Cloud Computing is a very promising concept of technology, but there is still a long way to go for security, governance, risk and compliance related issues to be formalized and streamlined with the changing times in the IT industry.

Wipro consulting services- Governance, Risk Management & Compliance practice have worked on the main concern areas of Cloud Computing – Governance, Risk & Compliance (GRC) Assessment and therefore have developed a “GRC Approach for Cloud Computing” .Its main focus is to list Threats, vulnerabilities, Risks that are associated to all three parts of Cloud Computing – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) & Software as a Service (SaaS) and suggest controls which have been assimilated from the best practices prevailing in the Industry. These controls have been placed in order to mitigate the risks in Cloud Computing and provide unified approach to handle and manage them.

This White paper targets on the GRC aspect of Cloud Computing and suggests methodology and techniques to tackle cloud security related problems in detail in the subsequent sections. Any organization who is a cloud consumer or a cloud service provider may adopt this approach to ensure cloud security in a holistic manner.

## **Benefits of Cloud computing & Problem Statement**

The objective of providing Cloud security to Cloud Computing is to justify the benefits associated to it. But the speculations revolving around Cloud computing can't be neglected as it ranges from basic data level security when it is stored at a third party location to Compliance or Security practice & Legislation.

There are series of changes taking place internally and externally for a business environment leading to increased level of complexity of threats and risks arising around it. However there are compelling benefits to Cloud Computing:

- Change from capital expenditure(CAPEX) to Consumption based Operational expenditure
- Go green with device & location Independence
- Scalability and flexibility without compromising customer value

Although these benefits offered by Cloud Computing are quite tempting for any organization as it has lead to the basic characteristics which have always been important: Cost Savings, High Availability, Flexibility, Agility & Efficiency.

The Problem comes in when we want to see the basic three pillars of Information Security Confidentiality, Integrity and Availability to be in place. We understand the cost of security solutions we deploy, but what about the cost of inaction, the cost of security failures to the business or the cost to the business of too much security? As we are moving from Language of Security to Language of Risk we need to evaluate these aspects and act accordingly.

## **Key speculations & problems faced by Cloud users in today's time**

Due to lack of proper understanding and application of related controls to ensure certain aspects of Confidentiality, Availability & Integrity (CIA) there have been lot of speculations and apprehensions for many Businesses' to use Cloud Computing as a tool for all the benefits mentioned above. As we are moving from securing IT Infrastructure to securing Information in terms of Confidentiality, Integrity & Availability we need to address the following concerns related to Information Security.

## **Threats, Vulnerabilities & Risks:**

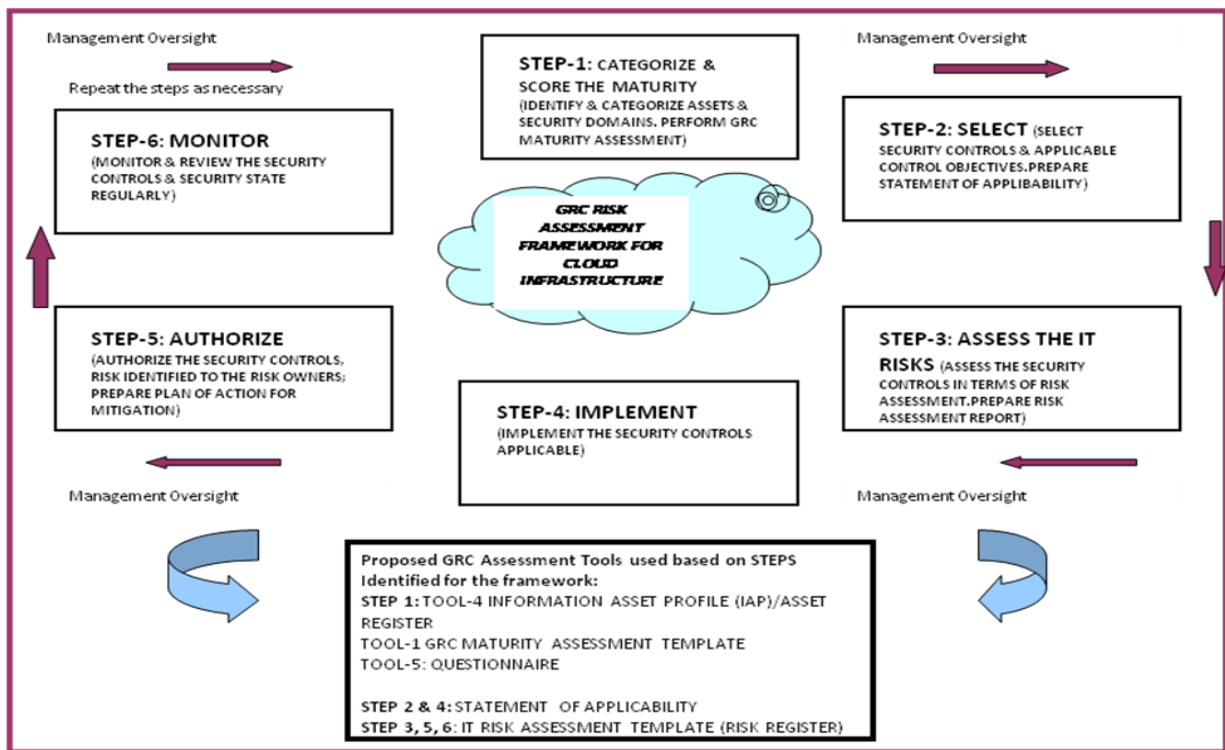
- Potential Loss of Control of Data once it is stored on Third Party Cloud.
- Possible leakage of Data & Confidential Information.
- Privacy Management.
- Availability, Reliability & Longevity of Cloud & Service providers.
- Rapidly growing volumes of Data.
- Stable level of Abstraction, Virtualization and Encapsulation.

- New Threat Environments.
- Adherence to Legal Laws and Regulations varying across the globe for Information Security.
- Intellectual Property Issues: Ownership and right to use.
- Ensure secure operations.

These are the major concerns which are enveloping everyone’s thought process in today’s time when it comes to Cloud Computing and Wipro Consulting Service-Governance Risk & Compliance has kept these into focus in order to develop the GRC Approach for Cloud Computing.

### Wipro Recommendation: Holistic Approach to cloud security- Governance, Risk Management & Compliance framework

Wipro Consulting Service-Governance, Risk & Compliance Practice (WCS-GRC) has developed GRC Assessment framework for Cloud Computing which is based upon the Industry Best practices and research on key Information security related issues over the years. This proven framework is helping Cloud Service providers, assessing cloud services and also checking self-readiness for cloud services. Overall WCS-GRC approach is a single unified set of controls with continuous monitoring process whose objective is to secure the Cloud in a step by step approach. This Activity begins with classifying & categorizing assets followed by identifying & selecting Control objectives and related controls to mitigate threat, vulnerabilities and risks to these assets. These control requirements may be mandated by government regulation such as Sarbanes-Oxley, by industry standards such as the International Organization for Standardization (ISO) 27000 series and the Payment Card Industry data security standard (PCI DSS), and even by organization own security best practices. These controls are mapped with individual standards and redundant or not applicable controls are removed accordingly. The Control framework so established is prioritized according to identified assets, risks and vulnerabilities.



**Figure-I: Wipro’s GRC Assessment Framework for Securing Cloud-A Six Step Approach**

needs. WCS-GRC has designed a 6 step approach to evaluate and assess the maturity, IT risks related to the services offered by cloud service provider under IaaS, PaaS, SaaS or EaaS with respect to Governance, Risk & Compliance. The same approach can be adopted by organizations for self assessment of their readiness to use the Cloud services from GRC Perspective.

This framework has been very carefully crafted and designed by referring knowledge base and expertise of GRC for Information security over the years and Industry Standards & Best Practices namely ISO 27001, ISO 31000, CobiT 4.1, ITIL v3.0, OCTAVE, NIST SP 800-30, SOX, SAS-70 and ISF.

There are few standards that can be directly combined and used to establish this security framework for Cloud Computing:

- SAS 70 Audit (Statement of Auditing Standards).
- Combined ISO 27001, ISO 31000, CobiT 4.1, ITIL v3.0 & NIST-SP 800 30 security best practices for GRC Maturity Assessment and IT Risk Assessment.

### **Wipro Identified GRC Domains:**

For performing the GRC Assessment of the cloud services or for the readiness assessment, WCS-GRC has identified the following GRC domains in order to cover all information security related aspects for Cloud Computing and the GRC assessment is done across all these identified domains.

- Governance & Enterprise Risk Management
- Compliance & IS Audits
- Legal regulations and laws
- Electronic Discovery (e-discovery)
- Information Lifecycle Management
- Identity & Access Management
- Policy Management
- Data Protection
- Encryption & Key Management
- Data Centers Management
- Incident Management
- Storage level Security
- Virtualization Security

These domains have been identified in order to understand the different areas that are involved with Cloud Computing Security in a holistic way. These are the key domains which are critical to any organization looking for an overall security which ensures that the data residing in public or private cloud is safe

## Wipro's GRC Assessment Tools used for Cloud security readiness for cloud consumers and cloud service provider GRC Maturity assessment:

“GRC Assessment Tools” from this part of the service includes a statement of applicability that documents the organization common control framework as well as a list of highly critical controls that require priority during follow-on assessments and remediation efforts.

This Statement of Applicability tool has been constructed for mapping different control standards and the GRC domains in order to do as-Is analysis and suggest missing controls. Key industry standards for Information Security used for it namely are ISO 27001, CobiT 4.1 and ITIL v3.0. These standards have not been used as it is in the manner they are already available; instead they have been handpicked accordingly specifically for Cloud Computing security.

ISO 27001:2005 Controls	Security Controls Identified to Preserve	Description of controls/Key Area	ITIL V3	CobIT 4.1	Remarks (Appl) for system
4.1.1 Management Commitment to information security	Trust & Fallacy Management	Business cases, in terms of knowledge, information, technology and regulatory needs	22.4.4F (number of systems management)	P03.3 (Higher Policy levels and regulations)	
4.1.2 Management Commitment to information security		Technology and other products and services	22.4.3.3 (Policies and practices)	P03.3 (Higher Policy levels and regulations)	
4.1.3 Management Commitment to information security		Provisioning of equipment, program and data protection to address		P03.3 (Higher Policy levels and regulations)	
4.1.4 Management Commitment to information security		Personnel security		P04.3 (IT service capabilities)	
4.1.5 Management Commitment to information security		Physical security			
4.1.6 Management Commitment to information security		Business classification of IT	22.4.1 (Classification of documents)	P04.4 (Data classification of the IT function)	
4.1.7 Management Commitment to information security		Configuration files	22.4.2.4 (Software configuration management)		
4.1.8 Management Commitment to information security		Organization of all aspects with respect to IT	22.4.3.4 (Software configuration management)	P04.3 (IT service capabilities)	

Figure 2: Statement of Applicability

The first step in the GRC Assessment is to perform the **Maturity Assessment** of the cloud services or readiness of the user to consume the cloud service, either ways the maturity assessment has to be done to check the maturity level of the cloud in terms of Governance, Risk Management & Compliance. This maturity assessment model has been designed to check the Cloud Security and at what maturity level it is. Thereby it would help in doing Current state Analysis and also show To-Be destination as in terms of maturity level required for Cloud Security. This maturity assessment also comprises of an overall assessment which shows key security areas and domains. It gives a score card in form of ratings and a spider web chart to show which parameter is required and falling short vice-versa.

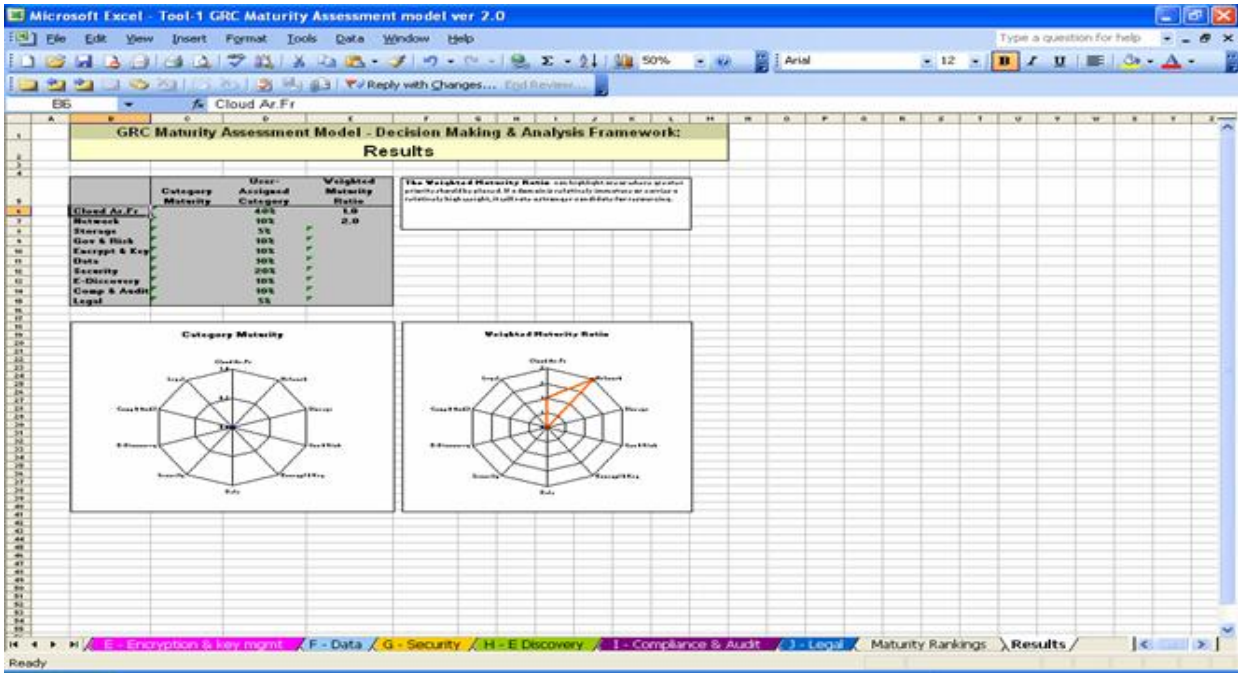


Figure 3: GRC Maturity Assessment Scorecard

In addition to the **Statement of Applicability and Maturity Assessment Score Card**, A **Risk Register** would be maintained which would keep track of identified assets as well as related Threats, Vulnerabilities, Risks and Mitigation plan and costs associated with each is managed. This Risk Register would clearly list out the Cloud assets classified under 4 main heads Virtual Information Assets, Physical IT Assets, IT Service Assets and Human Information Assets. This would also enlist associated Threats and Vulnerabilities on each Asset profile.

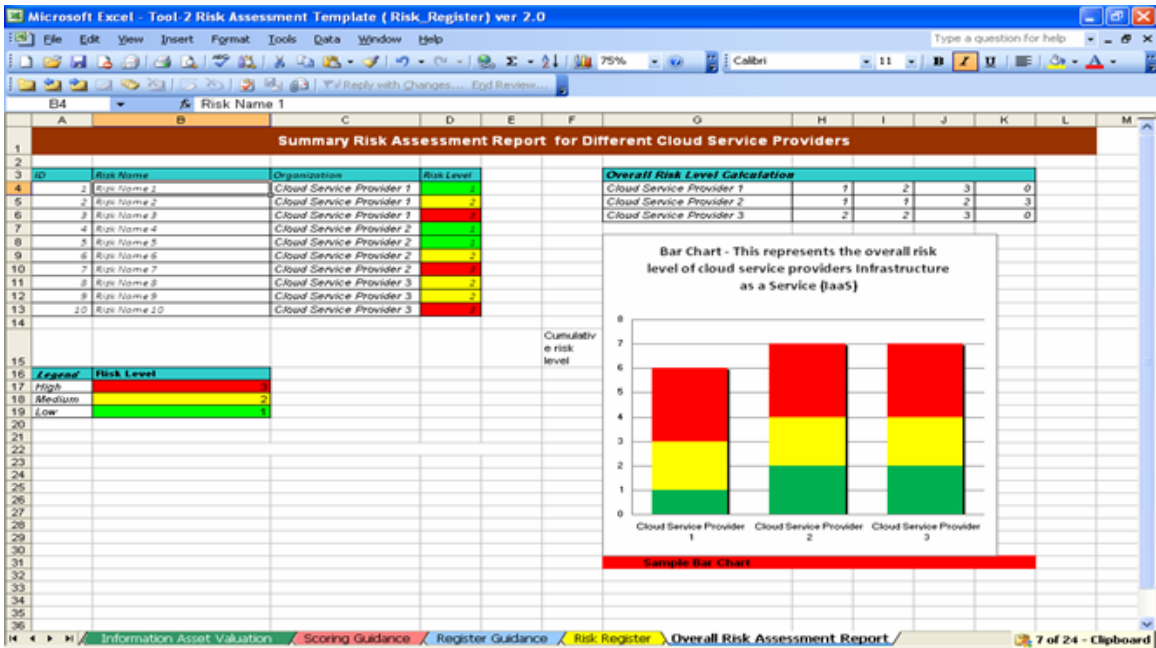


Figure 4: Risk Register

It is recommended as per best practice that penetration testing should be done to check the security for the given cloud along with third party audits in every six months to ensure compliance to GRC requirements and organization information security practices. Cloud consumers can perform Self Assessment or Third party assessment can be performed to check their readiness to use the cloud services from GRC perspective.

## **Wipro Recommendation: Top 4 Action steps to ensure that Cloud Service/Service Provider/Cloud Consumer is secured in a holistic way.**

- Step 1: Establish a GRC Assessment Framework by the method explained above and assess security levels of your Cloud/Cloud Service providers or cloud consumers can perform self-assessment to check their readiness.
- Step 2: Do a SAS 70 – Type I & Type II Audits to check the current status and for continuous monitoring.
- Step 3: Penetration testing to check the security layers and accordingly the weak Areas can be hardened to ensure security.
- Step 4: Third Party Audits/Assessments to check the Information Security Status and to establish continuous monitoring of internal controls.

## **Conclusion**

Cloud Computing is transformative phenomenon and becoming an emerging need or effective alternative in near future. Governance, Risk Management & Compliance is an imminent part of cloud computing to which ignorance won't help. The Structured approach to secure cloud and the consumers cloud integration points will make the customer feel confident to consume the cloud services. The changing environment from increasing complexities of a business has made it imperative to secure and mitigate risk in today's time. Therefore, to proactively act on it is important and doing so would bring in customer confidence and more innovations in this line of business.

## **Acronyms**

- CobiT 4.1: Control Objectives for Information Technology
- GRC : Governance, Risk & Compliance
- ISO 27001: International Organisation for Standards - Information Security Management Systems
- ISO 31000: International Organisation for Standards – Enterprise Risk Management
- ITIL v3.0: Information Technology Infrastructure Library
- NIST : National Institute of Standards & Technology
- IaaS: Infrastructure as a Service
- PaaS: Platform as a Service
- SaaS: Software as a Service
- SAS 70: Statement of Auditing Standards

## Key References

- Cloud Security Alliance – Security Guidance for critical Areas of Focus in Cloud Computing by Jim Reavis and Nils Phulmann
- ITIL v3.0 – Information Technology Infrastructure Library
- CobiT 4.1 – Control Objectives for Information Technology
- ISO 27001:2005 Standard for Information Security
- NIST-SP800-30 – Risk Management guide for Information technology systems by National Institute of Standards and Technology
- CobiT Mapping – Aligning CobiT 4.1, ITILv3.0 and ISO/IEC 27002 for Business Benefit by ITGI and OGC

## About the Authors

**Malini Rao** is a Senior Consultant with the Governance, Risk & Compliance Practice of Wipro Consulting Services and has over 8 years of experience in Information Security Consulting, IT Consulting & IS Audits. She can be reached at [malini.rao@wipro.com](mailto:malini.rao@wipro.com)

**Varun Kashyap** is a Consultant with Governance, Risk & Compliance Practice of Wipro Consulting Services. He focuses predominantly on Information Security, Enterprise Risk Management, Compliance Management, GRC Security Assessment Framework & IS Audits. He can be reached at [varun.kashyap@wipro.com](mailto:varun.kashyap@wipro.com)

## WIPRO CONSULTING SERVICES

Wipro Consulting Services (WCS) partners with you to transform your business through a combination of business insights, technology innovation and deep industry knowledge. Wipro Consulting offers Business Advisory, IT consulting and Program Management services designed to improve business performance, drive operational efficiency and maximize ROI.

With experts based in Europe, North America, India, Asia Pacific and the Middle East, our integrated Consulting, IT, BPO and Product Engineering services combine the benefits of expert proximity with global leverage to provide the technology edge and speed to your strategic programs. Wipro Consulting Services is a division of the Wipro Ltd (NYSE: WIT), a \$5bn enterprise that employs over 90,000 employees across the globe. Visit [www.wipro.com](http://www.wipro.com) for more details.

## ALL RIGHTS RESERVED

© Copyright 2009. Wipro Technologies. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Wipro Technologies. Specifications subject to change without notice. All other trademarks mentioned herein are the property of their respective owners. Specifications subject to change without notice.