
Cloud Adoption and Security in India Survey Report

November 2016

© 2016 Cloud Security Alliance - All Rights Reserved

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance “Cloud Adoption and Security in India Survey Report” at <https://cloudsecurityalliance.org/research/download>, subject to the following: (a) the Report may be used solely for your personal, informational, non-commercial use; (b) the Report may not be modified or altered in any way; (c) the Report may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Report as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance “Cloud Adoption and Security in India Survey Report” (2016).

DISCLAIMER

The views reflected in this article are the views of the authors and do not necessarily reflect the views of the global CSA and InstaSafe organizations or their member firms.

Acknowledgements

Managing Editors/Researchers

[Mickey Law](#)

[Ekta Mishra](#)

Designer

[Victoria Choi](#)

Supported by

[InstaSafe Technologies](#)

Table of Contents

Acknowledgements	2
Executive Summary	3
1. Introduction	4
2. Results	
2.1. Cloud Adoption in India	5
2.2. Cloud Security in India	11
3. Methodology	14
About	16

Executive Summary

Cloud adoption is an expanding part of organizations' IT strategies, and IT architects are growing more sophisticated in how they think about the cloud, but as of early 2015, relatively few organizations had truly advanced levels of cloud maturity^[1]. Despite the preconception that companies in the United States of America (USA) adopted technology earlier than its counterparts in Europe and Asia Pacific (APAC), the cloud adoption practices and priorities survey by the Cloud Security Alliance (CSA) in 2015 found the contrary. Results showed that organizations in the USA did not consider the cloud as a priority compared to those in APAC, where the cloud was suggested to be a key feature in business strategies.

From this survey, we have identified 2 pressing concerns and hope that through the publication of this report, the issues that have been identified will be rectified and continuously improved.

A lack of established industry standards within the Indian cloud computing industry is a lingering problem that the country faces. Cloud services offered in India by local providers are commonly proprietary to a great extent, which may pose challenges for cloud customers in case they want to develop a global IT strategy; not to mention moving from one cloud provider to another. In addition, the current state of relevant national standards in India

is neither compatible nor aligned with global standards. As a result, it does not support or scale well with the new demand for cloud services to be based in India, serving demands internationally. With a lack of standards and guidance to evaluate cloud service providers, Indian CIOs will not be able to adapt cloud strategy in their organizations against global business requirements.

Another key finding from the survey is that Indian organizations are extremely concerned about security, especially data sovereignty. Organizations are most worried about their data on the cloud. Data breach and data loss are major concerns of organizations from a cloud security perspective. While there is great interest in cloud-based solutions, apprehensions remain as to whether cloud services can ensure adequate protection of sensitive information. Specifically, respondents are concerned about the lack of strategy to address security issues in the cloud. Consequently, this will jeopardize the reputation of India being the global IT leader if these security concerns are not addressed and local cloud service providers are not aligned with global best practices. Fortunately, the government is acutely aware of these challenges and seems to be putting effort into addressing some of the weaknesses in the infrastructure, by announcing the launch of Digital India program in mid 2015.

[1] Cloud Adoptions Practices & Priorities Survey Report, Cloud Security Alliance, 2015

1. Introduction

The benefits for enterprises moving to the cloud are clear; greater business agility, data availability, collaboration and reduction of costs. More organizations are moving to the cloud. India based IT professionals have borne witness to a shift in the adoption of cloud computing. Governmental support, improved vendor offerings, and the emergence of global standards have all converged to drive cloud computing to become the top priority for many organizations.

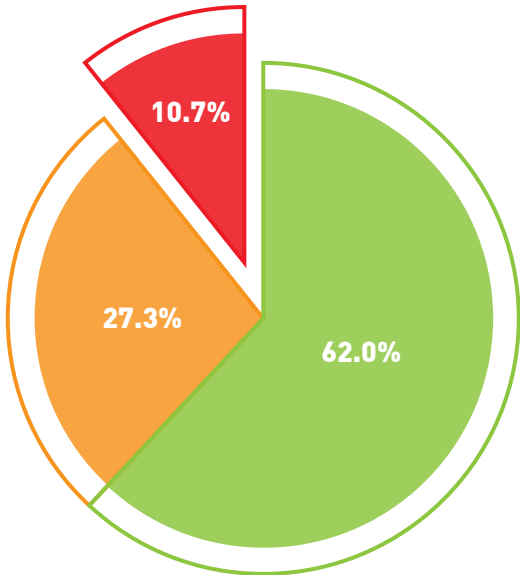
The “State on Cloud Adoption and Security in 2016: India” survey was circulated in an effort to understand and evaluate cloud computing trends in India. We hope to understand cloud adoption plans and usage from different industries in India and how cloud adoption can have an impact on organization business strategies and plans. This report is part of the CSA APAC cloud adoption state initiative, which aims to provide insights on cloud adoption in different APAC countries, to recognize APAC countries which are leading the cloud adoption trend as well as to identify the countries with opportunities for cloud computing adoption.

Results in this report is specific to cloud adoption in India, and statistics show that 88.3% of the respondents cite Software-as-a-Service (SaaS) as the most common form of cloud adoption. 62.0% mention that they are active cloud users, with some applications already on the cloud. Close to 27.3% say that they are evaluating moving to the cloud this year, and only 10.7% say that they have no plans of doing so. This indicates that cloud is present in India, replacing traditional IT outsourcing model and moving to cloud-based services such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and SaaS. These results are positive indications that Indian companies are ready to harness the cloud for more critical business applications. Examples are the use of data analytics on customer trends, Internet of Things (IoT), smart cars and other smart devices.

2. Results

2.1 Cloud Adoption in India

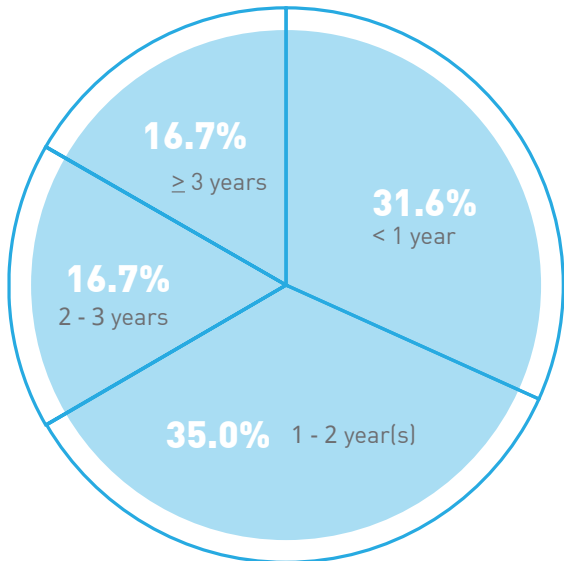
Cloud Adoption (Stages of Cloud Adoption)



- Active Users:**
We already have some of our applications and data on the cloud
- Potential Users:**
We are in the phase of evaluating multiple vendors prior to a trial
- Non Users:**
We have no plans to move our apps and data to the cloud

62.0% of the respondents are already active users of the cloud, 27.3% are evaluating moving to the cloud this year and 10.7% say that they have no plans on moving to the cloud yet. As such, cloud is going to be the major trend in India in the coming years. Indian government and organizations with businesses in India need to acknowledge this shift and should start refining measures to ensure they are prepared.

Cloud Adoption (Years of Experience Using the Cloud)

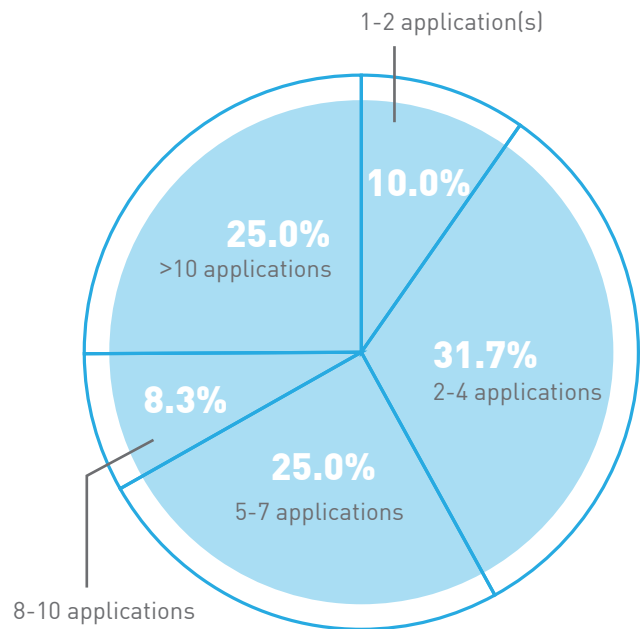


Out of the 62.0% who are active users, 31.6% mention that they have adopted the cloud for less than a year, 35.0% have been using a cloud service provider to host their applications and/or data for less than 2 years but more than a year. 16.7% express that they have been utilizing the cloud for more than 3 years. Currently, cloud is still very new in India and it is likely that many use cases, which already have mature models in other countries, have not been explored yet.

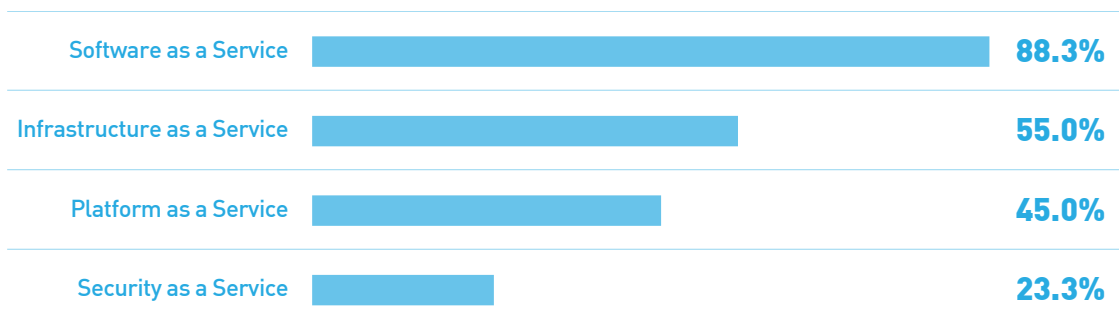
Number of Applications on Cloud

Statistics show that 25.0% of the Indian organizations have more than 10 applications on the cloud. 31.7% host 2-4 applications on the cloud and 10.0% have only 1-2 application(s) on the cloud.

Globally, an average organization uses 1,154 cloud services, with 174 of them being distinct collaboration services^[2]. There are 2 possibilities to the huge difference between the 2 sets of statistics. Firstly, Indian organizations are very conservative towards cloud adoption and secondly, individuals in India may be using cloud without even realizing it. Again, we are seeing that the cloud has not reached its full potential in India. Therefore, more efforts to educate Indian organizations are required to demystify the fear of using cloud.



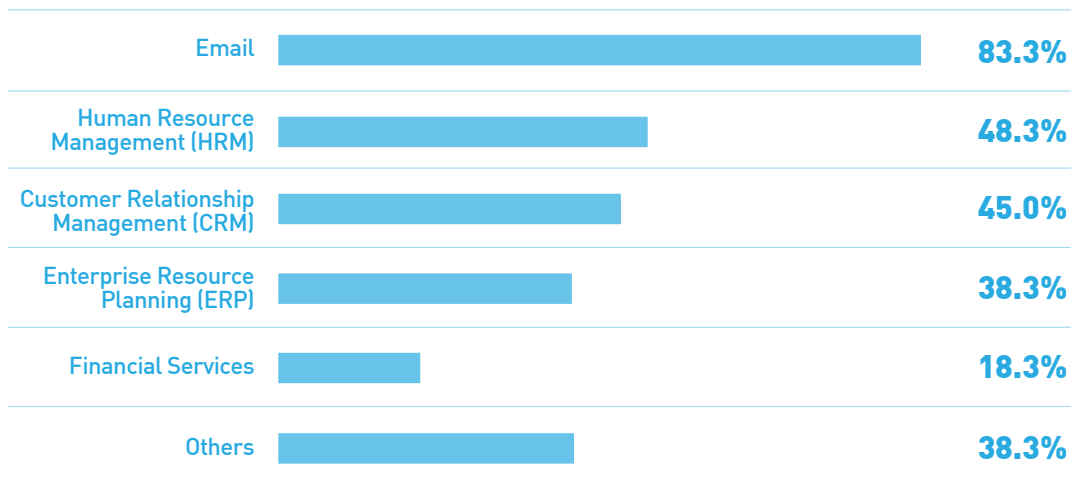
Cloud Service Delivery Model(s) Preference



With 88.3% of the organizations already adopting SaaS, it continues to be the top cloud service delivery model used in India. IaaS is the next most used cloud service model, with 55.0% adoption rate. A possible reason for the higher adoption rate for IaaS may be due to the ease of migration since IaaS is the most similar to traditional IT infrastructure.

[2] Cloud Adoption Risk Report, Skyhigh Networks, 2015

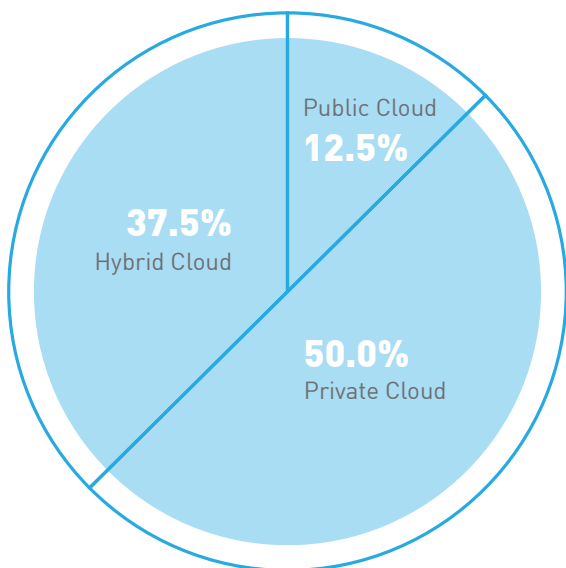
Applications Already on the Cloud



83.3% express that their organizations have moved Email to the cloud. HRM and CRM are the second and third applications which have been moved to the cloud, with 48.3% and 45.0% respectively.

Many organizations around the world are outsourcing applications to India, and most of these companies which provide outsourcing services use platforms such as CRM, HRM and ERP. When it is time to adopt the cloud, these applications will be moved first.







Cloud Deployment Model Preference



Indian organizations favor private cloud over public and hybrid clouds. Adoption rate for private cloud is 50.0%, while that of hybrid and public clouds are 37.5% and 12.5% respectively. Organizations may think that adopting private cloud will be more secure than adopting public and hybrid clouds, since private cloud can be customized for use by a particular organization only. However, whether it is more secure than the other two deployment models is questionable. Also, private cloud includes both internal and external hosting options^[3]. When private cloud is hosted on premise, it may not be fully utilizing the benefits provided by the cloud, which includes business agility.










[3] Cloud Security Alliance Guidance Version 3.0, Cloud Security Alliance, 2011

Main Cloud Functionalities Used

Business Application		88.3%
Storage		65.0%
Computing		50.0%
Virtualization		35.0%
Networking		13.3%
Others		8.3%

88.3% have been using cloud for business applications, 65.0% are using cloud for storage requirements. This indicates that cloud is mainly used for operational purposes in India and not for generating new revenue through innovative new cloud applications. Once more, we are seeing that the cloud has not achieved its full potential in Indian organizations.

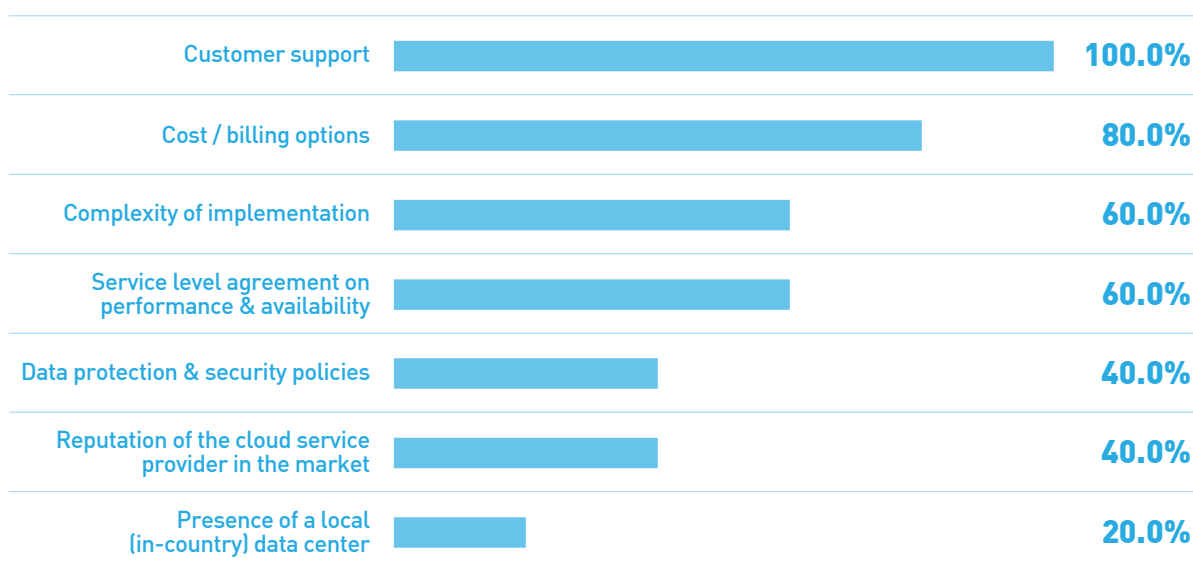
Reasons for Not Using Cloud

Lack of industry standards		60.0%
Not cost effective		60.0%
Difficulty integrating with environment		40.0%
Risk of data loss		40.0%
Risk of security breach		40.0%
Lack of control over infrastructure		20.0%
Risk of compliance violations		20.0%
Risk of service outage or degradation		20.0%
Others		20.0%

One of the 2 main reasons that user organizations are not moving to the cloud is the lack of industry standards. This may serve as a wakeup call for the Indian cloud security industry. Hopefully, this will urge providers to conform to existing international standards as well as encourage them to work towards developing local standards that are aligned internationally.









Another key reason is low cost effectiveness. When considering cloud adoption, cost is not the most fundamental, but rather the cloud's ability to provide more business agility. It is important for cloud service providers to highlight and demonstrate the potential value brought by cloud such as increased business agility.

Reasons for Choosing a Particular Cloud Service Provider



The primary concern when choosing a cloud service provider is customer support. Customers may be uncertain about adopting the cloud due to poor understanding of the cloud. This is the reason why continuous cloud/cloud security education is important to minimize such concerns. In addition, complying to standards and best practices that are globally recognized can help allay customers' concerns about moving to the cloud.

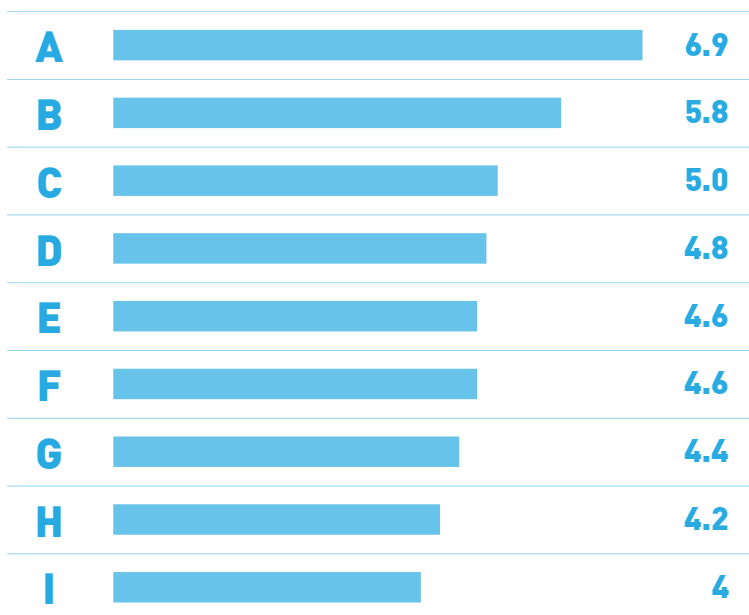
Market Dominance

Amazon Web Services (AWS)		46.7%
Microsoft Azure		41.7%
Google Cloud Platform		21.7%
Netmagic		13.3%
RackSpace		10.0%
CtrlS		8.3%
Tata Communications (InstaCompute)		5.0%
Others		20.0%

46.7% are using AWS and 41.7% are using Microsoft Azure. The top Indian cloud provider in this list is Netmagic, with 13.3% adoption rate. Overseas cloud providers are dominating the local market, and this can be due to the fact that they have more comprehensive offerings as well as economies of scale, which make their solutions more affordable. In order to compete, Indian organizations have to do more, and one of the first things to do is to comply with international best practices and standards.

2.2 Cloud Security in India

Concerns When Choosing a Cloud Service Provider



A Information security: Does the cloud service provider have information security measures as part of their infrastructure offering?

B Data ownership/custodian responsibilities: Is the data uploaded onto the cloud owned by the cloud service provider or you? Can the cloud service provider commit to security of your data?

C Disaster recovery/business continuity: Does the cloud service provider have a disaster recovery site or can they provide assurances of business continuity?

D Legal and contractual issues: Are the legal and contractual issues too complex?

E Technological stability: Is the cloud service provider using the latest technologies in their infrastructure and can they commit to maximum uptime?

F Performance: Can the cloud service provider commit to low latency, easy access and high performance?

G Geographical issues: Does the cloud service provider have a local in-country data center?

H Compliance with standards: Is the cloud service provider compliant with industry standards and can they prove it with relevant certifications?

I Contract lock-in: Does the cloud service provider have a minimum lock-in period to host your applications and data?

The key concern when choosing a cloud service provider is information security. To reduce security concerns, information security governance structure and processes should be implemented^[3].

[3] Cloud Security Alliance Guidance Version 3.0, Cloud Security Alliance, 2011

Key Hacking and Data Loss Concerns

Data breach: Data accessed by unauthorized personnel		79.2%
Data loss: Risk of losing data on the cloud due to factors like malicious attacks, natural disasters, data wipe		72.7%
Insider threat: Internal employee abusing cloud access to steal data and information		58.4%
Malware injection: Malicious code injected into cloud services compromising integrity of sensitive information		53.2%
Hijack of accounts: Accounts stolen through hacking		51.9%
Denial of service attacks: Make your servers and website unavailable to legitimate users		50.6%
Insufficient due diligence: Lack of clear policies and procedures within the cloud service provider's infrastructure		49.4%
Data-in-transit hacking: Data hacked and stolen while in transit from end point to the cloud (MITM Attacks)		45.5%

Organizations are most worried about data breach, with 79.2% of respondents expressing that they are concerned about data being accessed by unauthorized personnel. Data breach and its risks are not new to the information security world. In fact, risks of data breach have consistently been the top security industry concern^[3]. Reasons for data breach can be diverse; ranging from personal gains to state driven objectives.

It can be common for employees in India to job-hop. Ex-employees may steal confidential company information when leaving the organization and share it with the new firm. Multifactor authentication and encryption are 2 recommended solutions that can protect organizations against potential data breaches^[4].

Preferred Method for Secure Access

Cloud delivered models (Network Security-as-a-Service) to enable secure access		63.6%
On-premise hardware devices (Firewall/VPNs) installed in my network		57.6%
Multiprotocol Label Switching (MPLS) leased lines offered by carriers/telcos		13.6%

Looking at securing access to organization applications and data on the cloud, cloud delivered models (network SecaaS) appear to be in favor of the other two, which are on premise hardware devices and MPLS leased lines. This preference in adoption may be due to the fact that SecaaS is the cheapest option.

[3] Cloud Security Alliance Guidance Version 3.0, Cloud Security Alliance, 2011

[4] The Treacherous 12 - Cloud Computing Top Threats, Cloud Security Alliance, 2016

Factors Influencing Decisions To Implement A Security Solution

Quality of security	★	★	★	★	★	4.9
Amount of upfront investment required (capex investment)	★	★	★	★	★	4.8
Simplicity of solution	★	★	★	★	☆	4.2
Skilled manpower requirement to manage solution	★	★	★	★	☆	4.2
Continuous Annual Maintenance Charges (AMC) needed	★	★	★	★		3.7
Reduced operational complexity	★	★	★	☆		3.5
Time frame required to deploy solution	★	★	★			2.7

The 4 key factors influencing the choice of security solutions in an organization are the quality of security solutions, amount of upfront investment required, simplicity of the security solutions and manpower requirement needed.

Cost effectiveness has been the key consideration. Cloud, in nature, is an on demand service and SaaS are designed in a way that is simple to execute and thus, alleviating the need for complex solutions. Moreover, subscribing to a cloud solution, especially SaaS, put the onus of placing the right professionals onto the job to the service providers. In other words, it will be the providers' responsibilities to make sure that their engineers and architects are well trained and certified.

The providers should reference the Certificate of Cloud Security Knowledge^[5] (CCSK) as the key baseline for competency of the employees. Last but not least, to ensure that cloud solutions have the right security controls in place, customers should always ask for certifications such as the CSA Security, Trust and Assurance Registry^[6] (STAR) from their solution providers. This will attest the capability and competency of the providers.

















[5] Certificate of Cloud Security Knowledge (CCSK)
<https://cloudsecurityalliance.org/education/ccsk/>

[6] CSA Security, Trust & Assurance Registry (STAR)
<https://cloudsecurityalliance.org/star/>

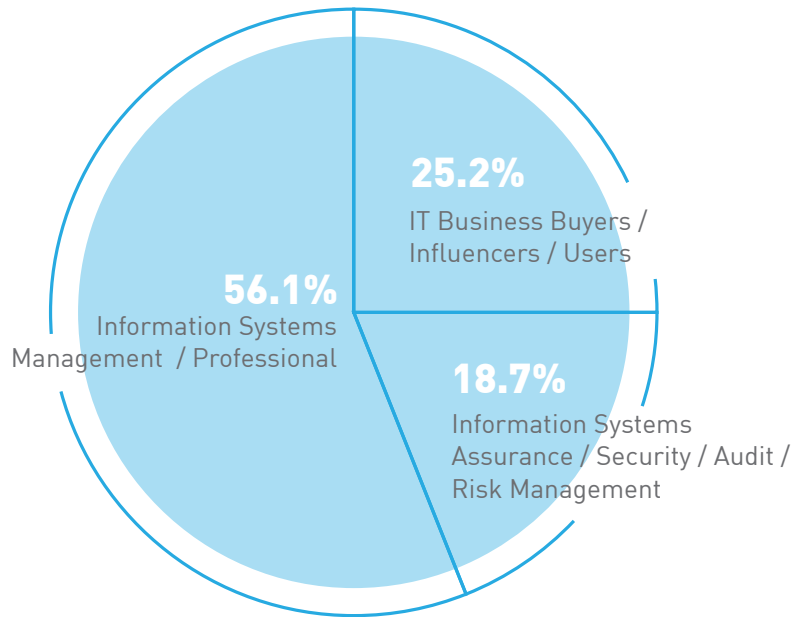
Methodology

The survey was conducted through an online questionnaire for a period of 2 months. The survey attracted 123 respondents and they came from various industries in India.

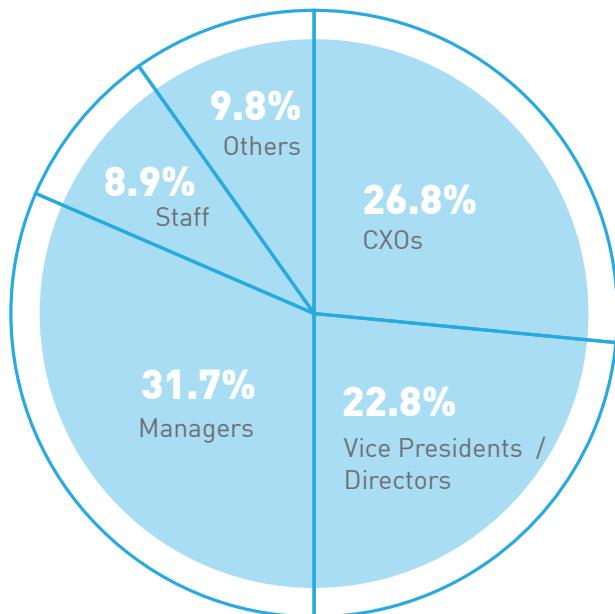
Industry

Technology		27.6%
Banking and financial services		9.8%
Manufacturing		9.8%
Consulting / professional services		7.3%
Retail / wholesale		6.5%
Telecommunications		5.7%
Insurance		3.3%
Communications		2.4%
Health		2.4%
Hospitality		1.6%
Transport		1.6%
Utilities & energy		1.6%
Chemical & pharmaceuticals		0.8%
Consumer goods		0.8%
Government		0.8%
Others		17.9 %

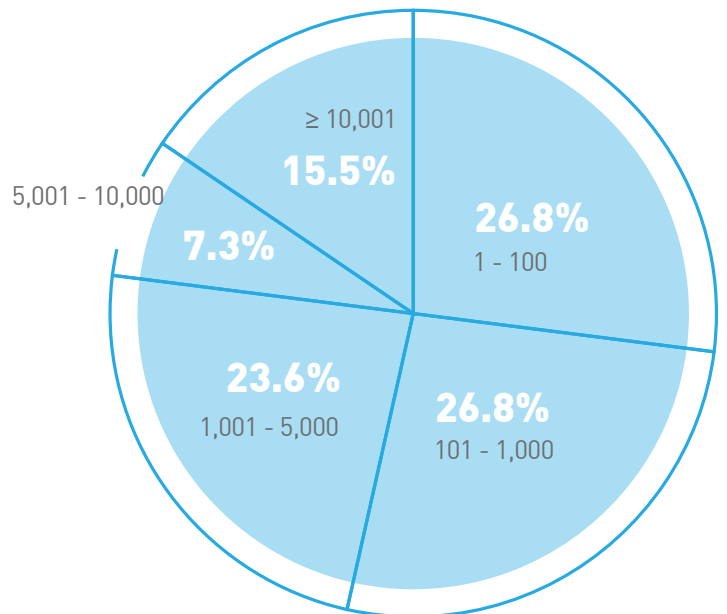
Professional IT Personnel



Designation



Enterprise Size (Employees)



About



The **Cloud Security Alliance (CSA)** is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

For more information, visit <https://cloudsecurityalliance.org> and follow us on Twitter @cloudsa.



InstaSafe Technologies is a leading Cloud based Security-as-a-Service solution provider delivering comprehensive and uncompromising protection to mobile and remote workers enabling them to safely and securely access enterprise apps, email and web from anywhere on any network.

For more information, visit <http://www.instasafe.com> and follow us on Twitter @instasafe.