Cloud Adoptions Practices and Priorities in the Chinese Financial Sector: **Survey Report**

October 2016

CSA cloud security alliance®

Acknowledgements

Managing Editors/Researchers

Mickey Law

Lynne Yang

Special Thanks

Ernst & Young (China) Advisory Limited (EY)

CSA Shanghai Chapter

Table of Contents

Executive Summary

The Financial Services Institution (FSI) industry has never been an early adopter of technology. Furthermore, it is also one of the most heavily regulated industry internationally. However, with the improvement of Cloud security over the years, many FSIs have become more confident in embracing it. Having seen this trend, the Cloud Security Alliance (CSA) and EY China Advisory have jointly conducted a survey, part of the result related with the FSI are have been used by the CSA for this report, to provide a clearer picture of Cloud adoption and to identify potential gaps that are holding back the adoption of Cloud within the FSI sector.

In this report, we have identified 3 states of Cloud in the FSI industry in China.

47.9% of the FSIs in China say they are developing a Cloud strategy, 43.8% say they have developed a Cloud strategy, but only 8.3% say they have a strict no Cloud policy.

54.2% mention that no Cloud service data security and compliance regulations are predetermined in their organization. This implies that over half of the organizations do not feel the need to define a strategy to address Cloud service data security and compliance regulations within the organization.

37.5% of the respondents say that the top Cloud threat in their organization is the lack of security management leadership. When there is a lack of emphasis on Cloud services regulations and requirements by the organization, it is almost a direct indication that the C-level management will do little to prioritize the initiative.

Due to the lack of commitment at the senior level, 63.5% of all Cloud computing and cybersecurity professionals indicate they have not participated in or organized any Cloud application development or Cloud security related training. It is important to note that 47.9% of the FSIs in China are developing a Cloud strategy and 43.8% of the FSIs in China already have a Cloud strategy in place. As such, it is worrying to know how these strategies are formulated. Firstly, there is a lack of management oversight and secondly, close to 65.0% of the Cloud computing and cybersecurity professionals are not trained in Cloud security. This combination is a recipe for catastrophe.

1. Introduction

We circulated the "Financial Services Industry Cloud Adoption Survey: China" survey to IT and security professionals in the Financial Services Institutions (FSIs) in China. The goal was not only to raise awareness around Cloud service adoption, but also to provide insight into how finance, government, insurance, and security decision makers take action in their organization within China. These actions included consolidating and standardizing the most secure Cloud services, knowing what policies would have the most impact as well as understanding where to focus for educating users.

The main topics discussed in the survey are:

- What are the approaches to Cloud computing that FSIs are using in China?
- What are the policies that the FSIs are using in their private Cloud?
- What are the corporate risk assessments of Cloud computing in the FSIs in China?
- What features would the FSIs appreciate from Cloud providers?
- What are the primary reasons for adopting Cloud computing in the FSI industry in China?

Key findings include:

Cloud Adoption

Cloud adoption in the FSIs has become prevalent now. 47.9% of the FSIs in China say they are developing a Cloud strategy, 43.8% say they have developed a Cloud strategy. Of the 8.3% who say they have a strict no Cloud policy, 50.0% say it is due to high cost and 50.0% say it is due to the high security risk associated with using the Cloud. For organizations which are already using the Cloud, IaaS best suits the organization's current Cloud service usage, followed by SaaS and PaaS.

81.2% of the FSIs in China say that up to 75.0% of the applications in their organization will be on Cloud in the next 12 months. The main factors affecting adoption have indicated to be the Cloud's ability to use and allocate on-demand; easy to expand and increasing agility. Other key factors for the FSIs in China to adopt Cloud include lower one time spending and operating costs, big data management and deep data mining, secure data storage for disaster recovery, and the presence of professional providers which deliver better and more stable services. For organizations which have adopted Cloud services or are interested in adopting Cloud services in the next 12 months, project management is expected to be the most sought-after Cloud service, followed by data storage and big data services.

From the figures shown, Cloud computing has become a mature area within the FSIs, with up to 75.0% of the applications ready to go into the Cloud in the next 12 months. Based on the statistics, this suggests that Cloud will be replacing traditional banking platform as the basic IT platform by 2017. As a result, FSIs in China will be utilizing their investments by building more applications which will harness the power of Cloud to draw business gains.

IT Security Budgets

When the amount of IT security spending relative to the average annual revenue in the past 3 years is questioned, 37.5% of the FSIs express that they use less than 10% of their average annual revenue on IT spendings and 29.2% of the FSIs reveal that they use 15-20% of their average annual revenue on IT spendings. This results show that the overall IT spendings relative to average annual revenue is low. In fact, according to EY 2015 GISS report[1], "69% say their information security budget needs to rise by up to 50% to protect the company in line with management's risk tolerance."

[1]: EY's Global Information Security Survey 2015, EYGM Limited, 2015

Cloud Computing And Cybersecurity Skills

63.5% mention that the percentage of Cloud computing and cybersecurity expertise and skilled personnels in their IT department is between 0-10%. 20.8% say the percentage range in their organization is between 11-20%. Among all the Cloud computing and cybersecurity professionals, 63.5% of them have not participated in or organized any Cloud application development or Cloud security related training.

As more organizations are choosing Cloud services, it is important to ensure that IT security or cybersecurity professionals have the right set of skills for their jobs. Consumers tend to be more sensitive when it comes to finance related matters and therefore it is crucial to ensure that IT security or cybersecurity employees have the correct level of capabilities for their jobs.

37.5% say that the top Cloud threat in their organization is the lack of security management leadership. When there is a lack of emphasis on Cloud services regulations and requirements by the organization, it is most likely that the C-level management will do little to prioritize the initiative.

From a bird's eye view, with 47.9% of the FSIs in China developing a Cloud strategy, 43.8% of the FSIs in China already having a Cloud strategy in place, top Cloud threat being a lack of security management leadership, and 63.5% of the Cloud computing and cybersecurity professionals not having any Cloud computing or cybersecurity training, it is worrying to know how the Cloud strategies in the FSIs are formulated. Consequently, this may create severe disaster for these FSIs. Hence, there is an urgent need for FSI regulatory bodies and senior management within the sector to pay more attention to Cloud security issues.

Cloud Service Compliance and Regulations

54.2% mention that no Cloud service data security and compliance regulations are predetermined in their organization. When asked the data protection and privacy concerns in Cloud, lack of data control and governance is believed to be one of the top 3 concerns that the FSIs in China have. Enhancing transparency and implementing effective audit controls are on the top list of functions/services that FSIs will expect their Cloud service provider/s to provide.

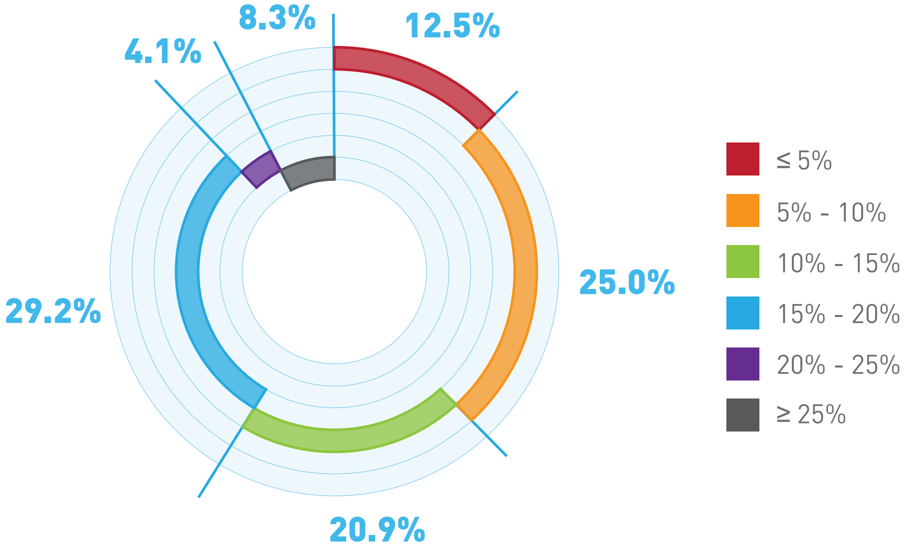
Moreover, safety, reliability and compatibility are the most important features that the FSIs are most concerned about when they are selecting a Cloud service provider. Safety refers to the presence of authoritative security certifications and an auditable overall management and control. Reliability refers to the high availability and the capability to minimize impacts on day-to-day business. Compatibility refers to the associativity with mainstream applications and systems.

Statistics from this survey also shows that FSIs in China take national and international standards/certifications into account when they choose a Cloud service provider. National standards such as the Trusted Cloud Service Assessment, the Administrative Measures for the Graded Protection of Information Security and GB/T 220800 - Information Security Management System Requirements and International Standards such as ISO 27001 and CSA STAR Certification are the main standards and certifications that the Chinese FSIs are paying attention to.

2. Results

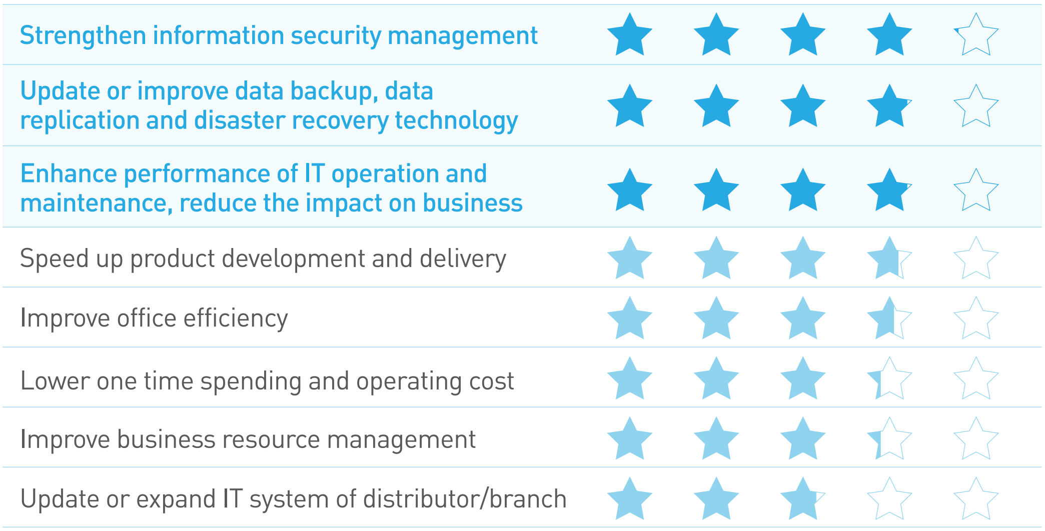
2.1. Background Information

Organization IT Spending V.S. Organization Average Annual Revenue in the Past 3 Years



In the past 3 years, 29.2% of the FSIs have IT spendings at 15% - 20% of the average annual revenue of the entire organization. 12.5% say that their IT spendings are less than 5% of the average annual revenue while 8.3% say that their IT spendings are more than 25.0% of the average annual revenue.

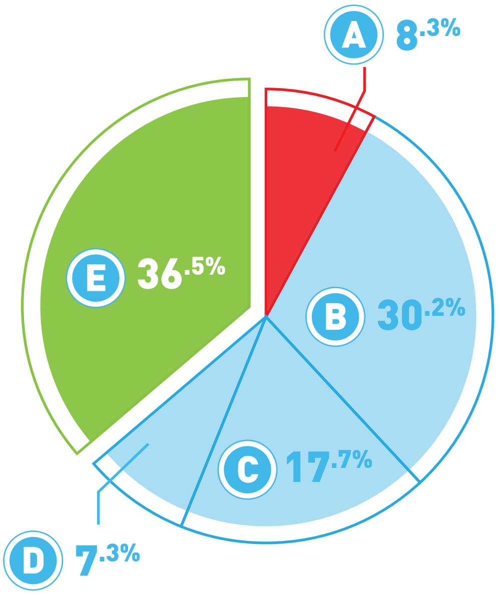
Priorities in IT Strategy Roadmap



FSIs are more likely to prioritize strengthening information security management in their IT strategy roadmap and are least likely to update or expand IT system of the distributor/branch as part of their IT strategy roadmap.

2.2. Financial Services Industry Cloud Adoption in China

Organizational Approach to Cloud Computing



A. We are not planning to adopt Cloud policy at the moment

B. We are developing a Cloud strategy, but **not included** in the overall IT or business strategic planning

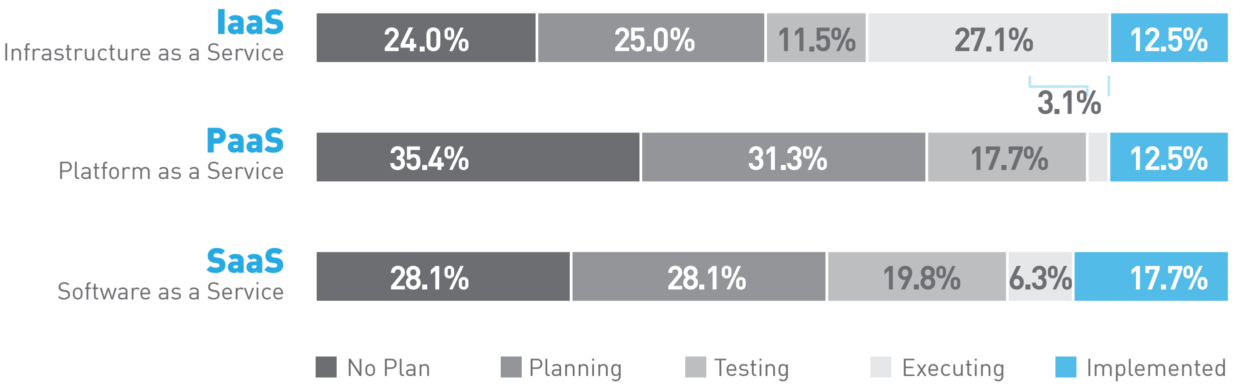
C. We are developing a Cloud strategy, and **included** in the overall IT or business strategic planning

D. We have developed a Cloud strategy, but **not included** in the overall IT or business strategic planning

E. We have developed a Cloud strategy, and **included** in the overall IT or business stratgic planning

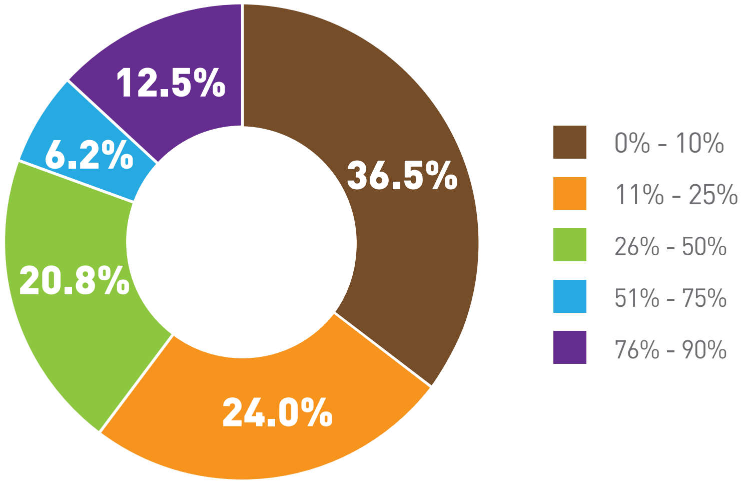
36.5% express that they have developed a Cloud strategy and have it included in the overall IT or business strategy planning. 7.3% mention they have developed a Cloud strategy but have not had it included in the overall IT or business. In total, more than 91.0% state that they either have already developed a Cloud strategy or are planning to develop one.

Current Cloud Service Usage



Although the ratio of FSIs using IaaS, PaaS and SaaS does not suggest a huge difference, most express that they are using IaaS, followed by SaaS and PaaS.

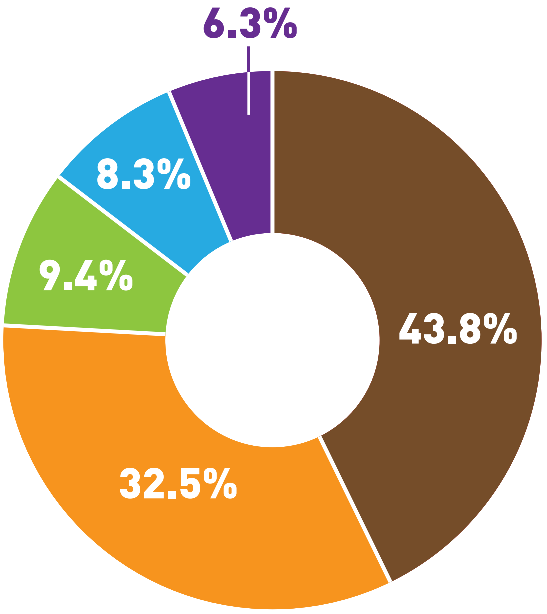
Percentage of Applications on Cloud in the Next 12 Months



In the next 12 months, 36.5% indicate that 0-10% of applications within the organization will be on Cloud. More than 80% state that 0-50% of the applications will be on Cloud. 18.7% will have 51-90% of applications on Cloud while no organization will choose to put more than 90% of their applications on Cloud.

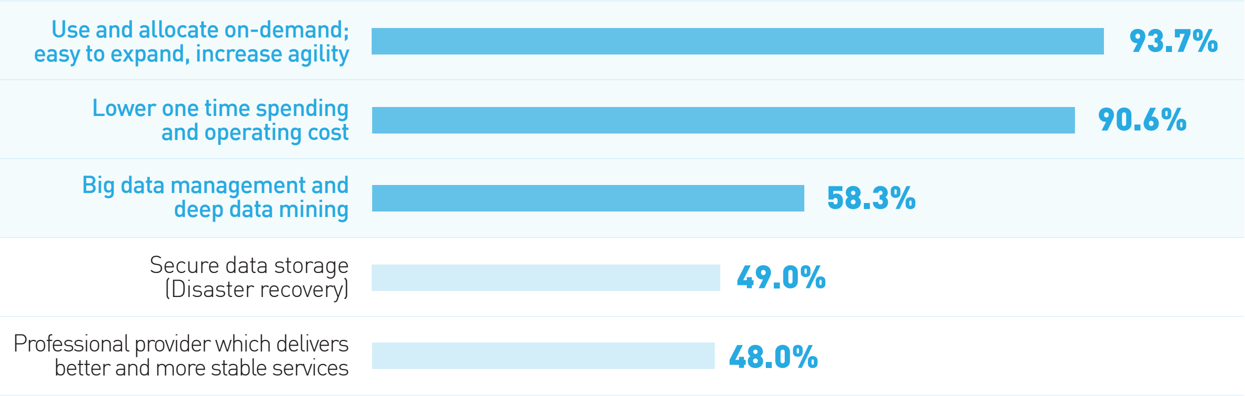
Type of Cloud Deployment Models Used/Planning to Be Used

- 🟫 Private Cloud (Cloud infrastructure that is provisioned for exclusive use by a single organization or an individual)
- 🟧 Hybrid Cloud (Cloud infrastructure that is a composition of two or more distinct Cloud infrastructure)
- 🟦 Public Cloud (Cloud infrastructure that is openly used by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combinations of them)
- 🟪 Community Cloud (Cloud infrastructure that is for exclusive use by a specific community of consumers from organizations that have shared concerns. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises)
- 🟩 Others

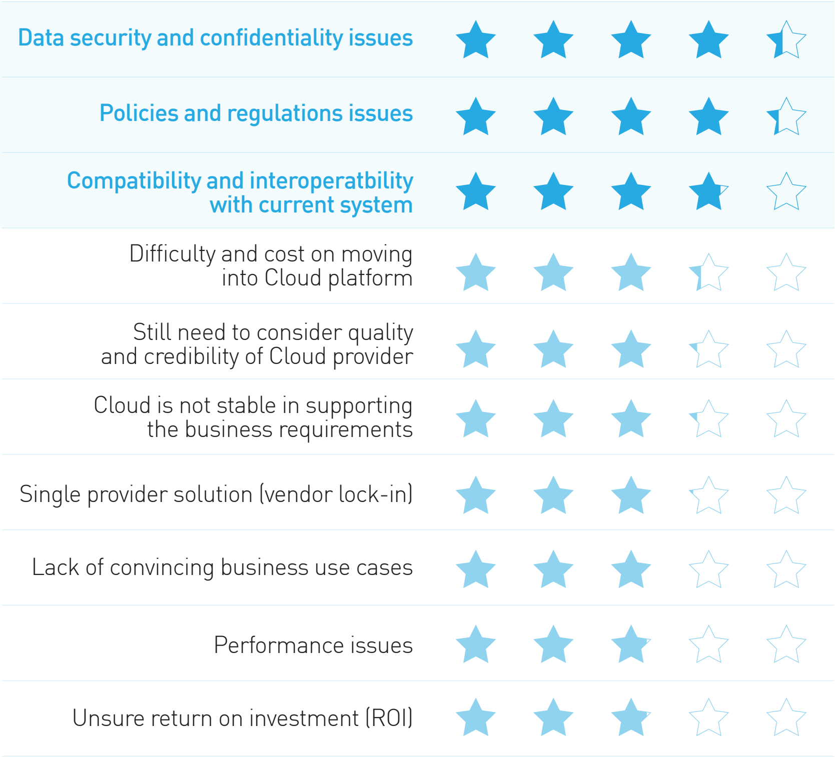


Out of all the organizations that are using or are planning to use Cloud deployment models, 43.7% indicate they are using private Cloud, while 32.5% say they are using hybrid Cloud. Community Cloud comes in at the bottom of the list, with only 6.3%.

Top 5 Most Important Cloud Adoptions

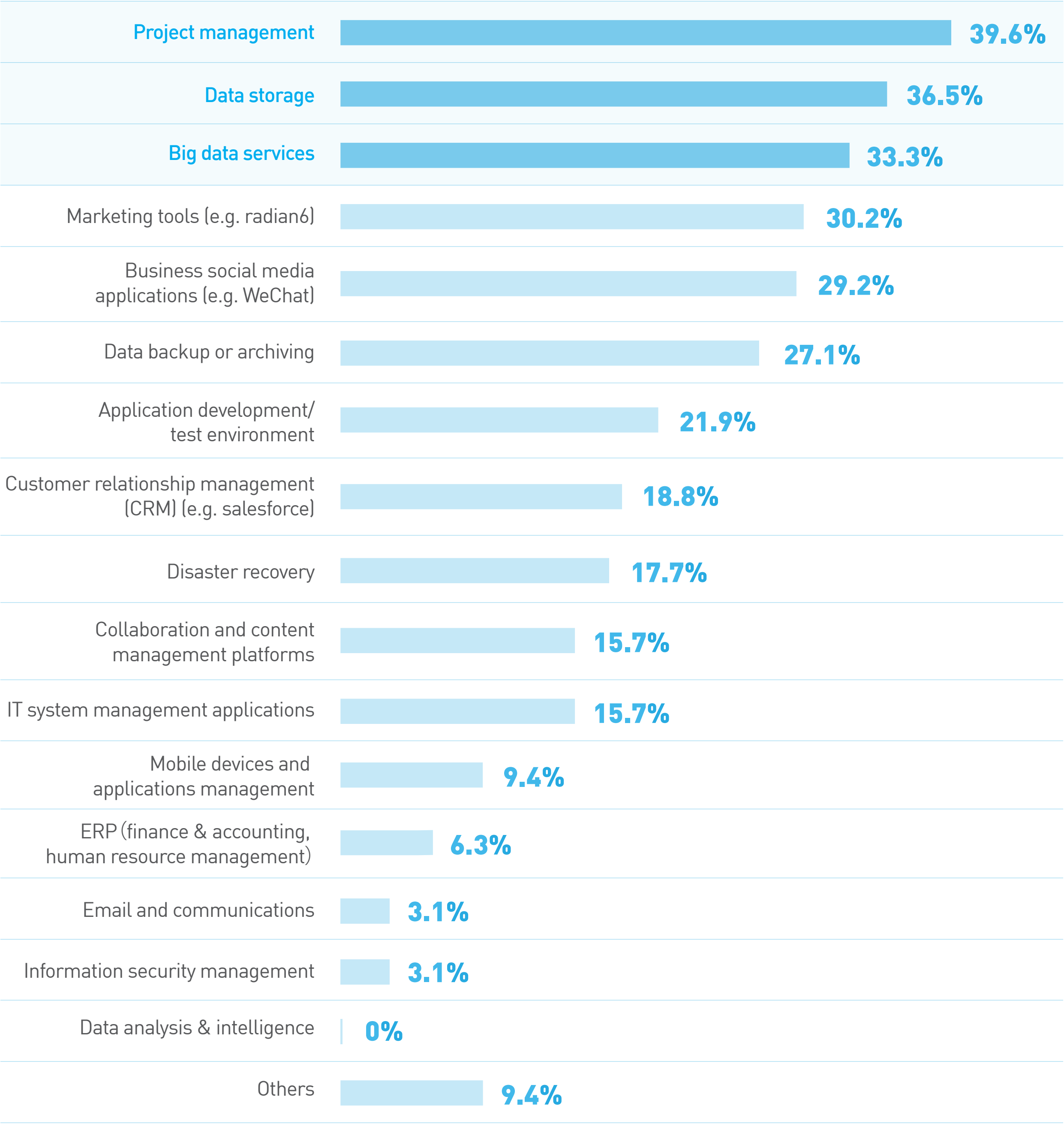


Main Concerns While Using Cloud



The main concerns in the FSIs are data security and confidentiality, and policies and regulations issues. Compatibility and interoperability with current system is the third most concerned factor on the list. Performance issues and uncertain return on investment (ROI) are of the least concerned for the Chinese FSIs.

Cloud Service Adoptions Now and in Future

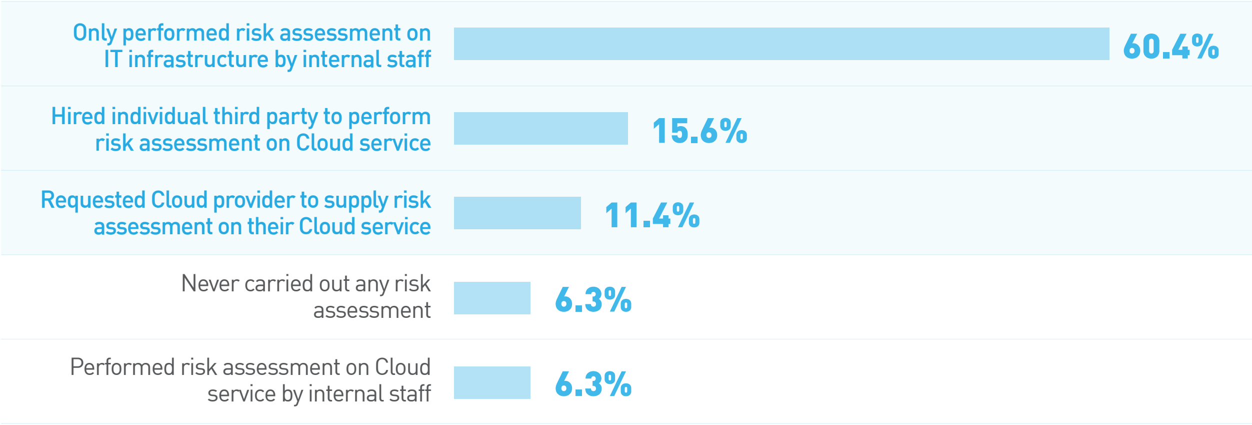


The top 3 Cloud services the FSI China industry is adopting or is interested in adopting in the near future are project management, data storage and big data services, statistics are 39.6%, 36.5% and 33.3% respectively. These results are similar to a report[2] published by CSA, where cloud adoption of projected management, data storage and big data services are at 41%, 41% and 28% respectively. On the other hand, data analysis & intelligence, email and communications, and information security management are the least interested adoptions, with 0%, 3.1% and 3.1% take-up rate respectively.

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

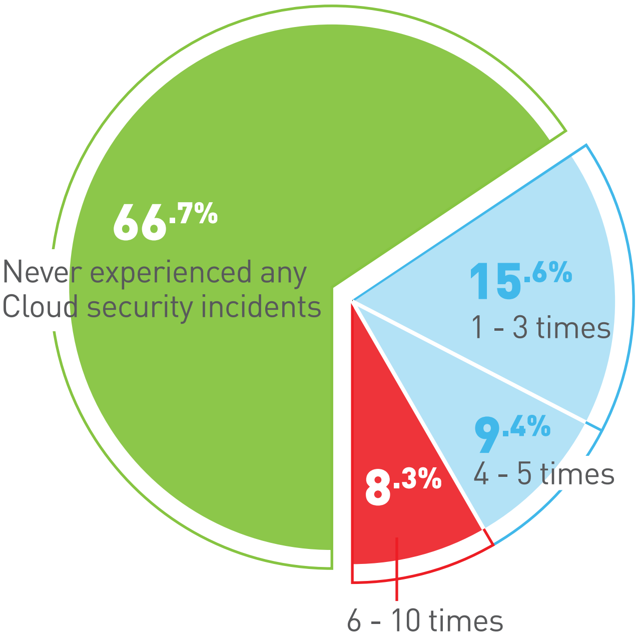
2.3. Financial Services Industry Cloud Security in China

Risk Assessment Activities in the Last 3 Years



In the past 3 years, 60.4% state that their organization only performed risk assessment on IT infrastructure and 6.3% state they have never carried out any risk assessment or performed risk assessment on Cloud service by their internal staff.

Security Incidents Related to Cloud in the Last 12 Months



66.7% of survey respondents mention that their organization has never experienced any Cloud security incidents in the past 12 months. 15.6% indicate a 1-3 times encounter with Cloud security incidents, 9.4% indicate a 4-5 times encounter with Cloud security incidents, and 8.3% mention a 6-10 times encounter with Cloud security incidents. However, it is possible that some of these security incidents may not be related to Cloud, as we often see IT managers mistake general IT security incidents as Cloud security incidents.

Type of Security Incidents Occurred

37.5%

- Data loss
- Data inaccessible
- Unauthorized access

12.5%

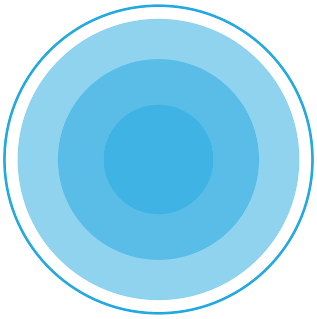
- Malicious software
- Services abuse

25.0%

- Others

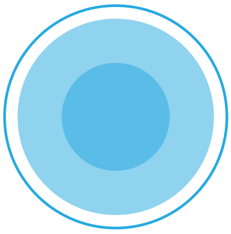
Results show that 3 incidents happen most frequently in FSI China and they are data loss, data inaccessibility and unauthorized access. Less frequent security incidents include malicious software and services abuse.

Top Cloud Threats



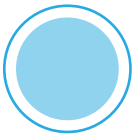
37.5%

- Lack of security management leadership



25.0%

- Users are easily exploited by phishing because of the lack of security awareness

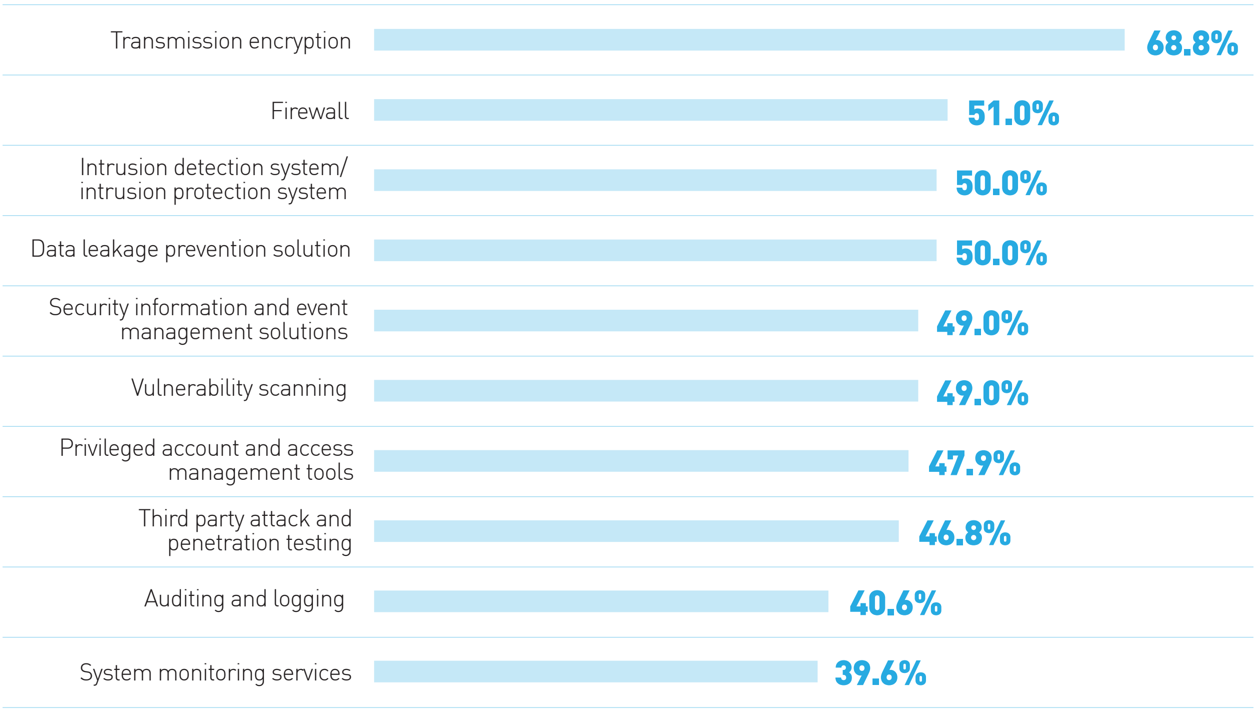


12.5%

- Lack of intrusion detection mechanism
- Lack of security assessments on Cloud services provided by Cloud service providers
- Lack of user permissions control

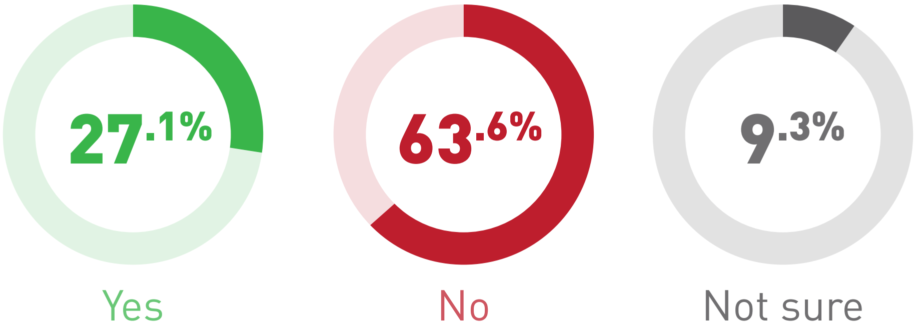
37.5% state that the top Cloud threat in their organization is the lack of security management leadership. 25.0% think users are easily exploited by phishing because of the lack of security awareness. 12.5% think the lack of intrusion detection mechanism, lack of security assessment on Cloud services provided by Cloud service providers, and lack of user permission control are the top threats.

Top 10 Measures Used to Address Cloud Security Concerns



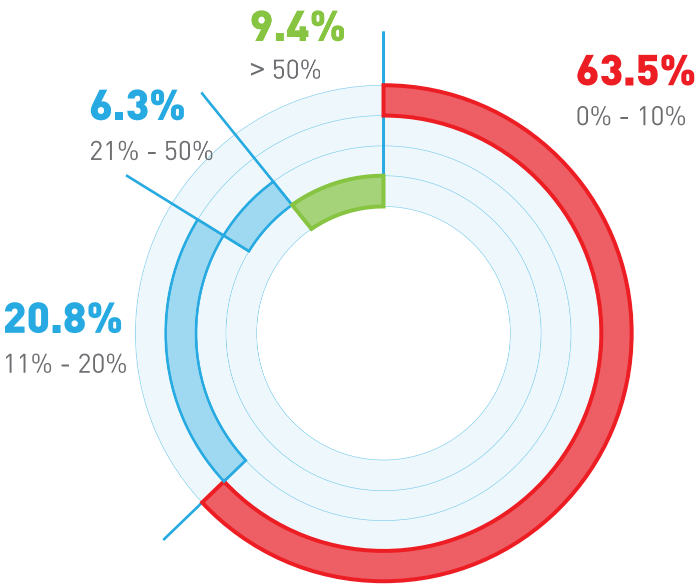
All FSI respondents express that they use some kind of measures to address Cloud security concerns. More than 68.0% of them mention they use transmission encryption. The least popular of all 10 measures is system monitoring services, with 39.6% take-up rate.

Cloud Application Development/Cloud Security Related Training



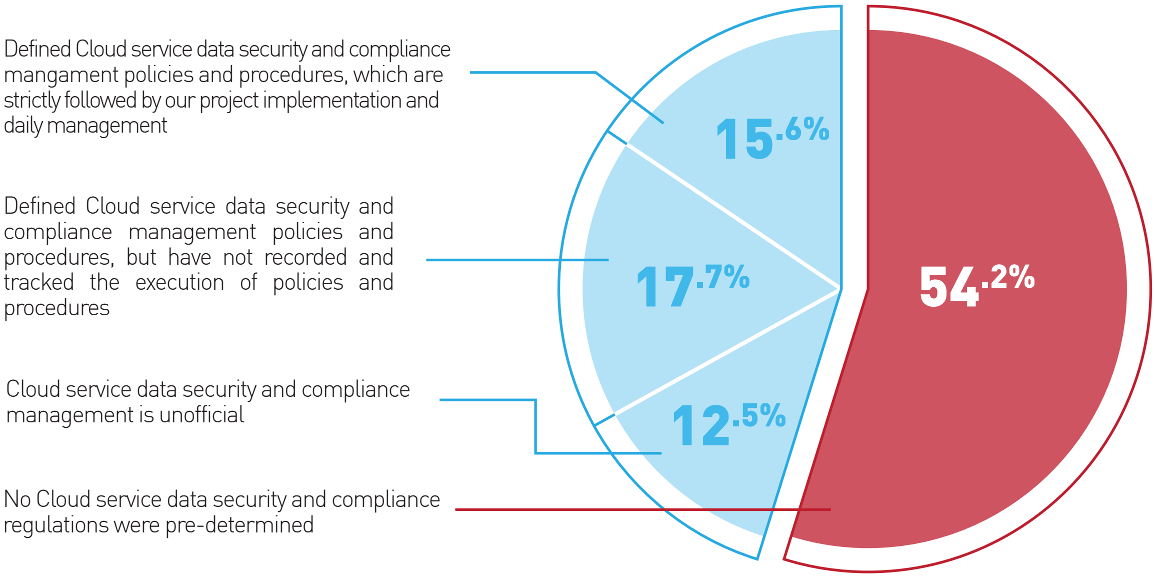
Over 60.0% say that their organization has never participated in or organized any Cloud application development or Cloud security related training. Only 27.1% of them has given a positive reply in this survey question.

Percentage of Cloud Computing Professionals in IT Departments



63.5% of IT departments hired none or only up to 10% of Cloud computing professionals. The proportion of Cloud computing and cybersecurity expertise and skilled personnel in IT departments is between 0-10%. Only 9.4% indicate a greater than 50% Cloud computing professional hiring rate in their IT department.

Corporate Policies and Procedures



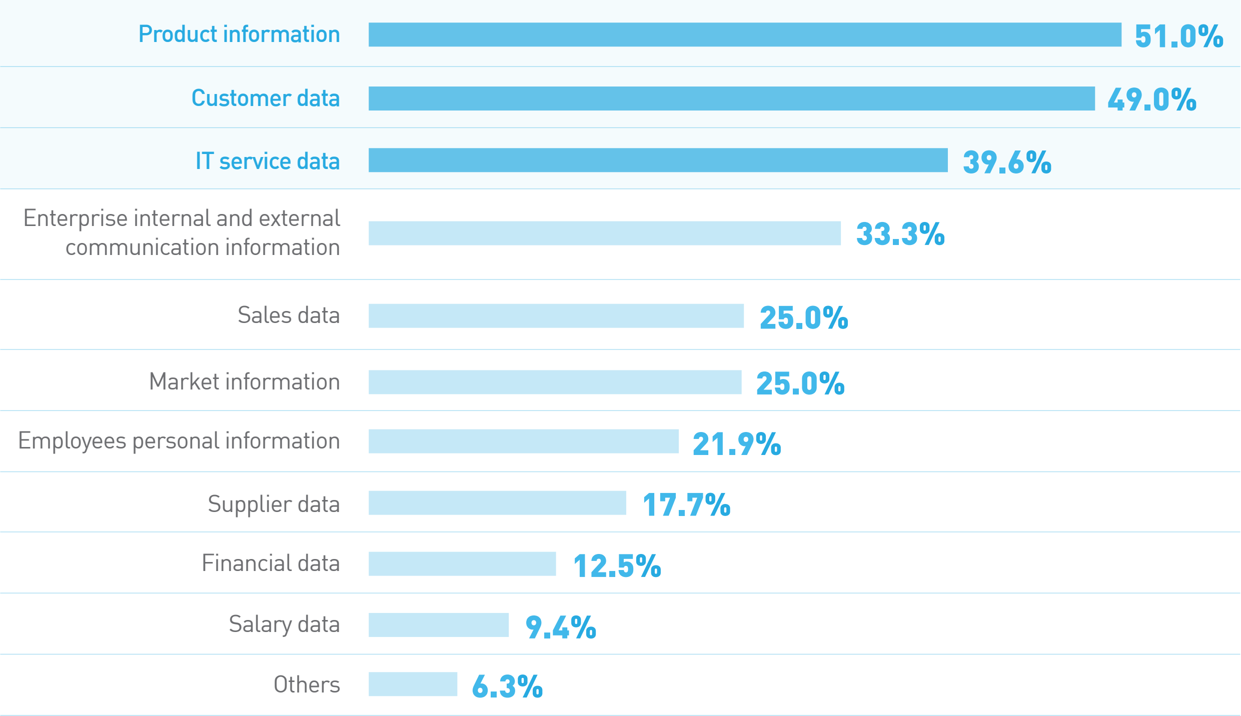
More than half (54.2%) of the organizations in the FSI sector mention no Cloud service data security and compliance regulations are pre-determined within the organization. 17.7% say that there is a defined Cloud services data security and compliance management policies and procedures, but they have not recorded and tracked the execution of policies and procedures. Only 15.6% say that there is defined Cloud service data security and compliance management policies and procedures which are strictly followed by project implementation and daily management. 12.5% mention Cloud service data security and compliance management is unofficial.

Cloud Deployment Models V.S. Security Classifications

	Public Cloud	Community Cloud	Private Cloud	Hybrid Cloud	All Not Allowed
Secret	6.3%	3.1%	33.3%	15.6%	44.8%
Limited	12.5%	6.3%	42.7%	24.0%	17.7%
Internal Use	14.6%	12.5%	53.1%	34.4%	6.3%
Public	53.1%	21.9%	25.0%	34.4%	6.3%

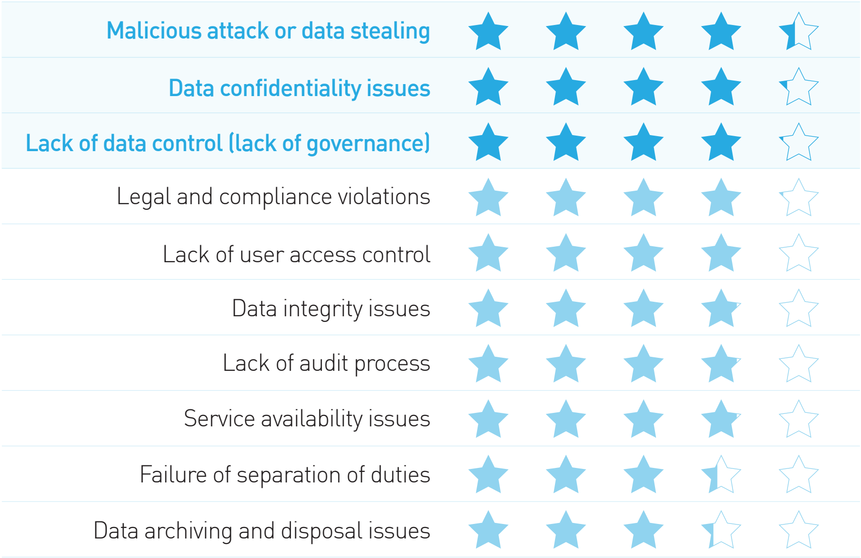
The table above shows the adoption percentages between the different Cloud deployment models and their corresponding security classifications.

Data Types Used/To Be Used



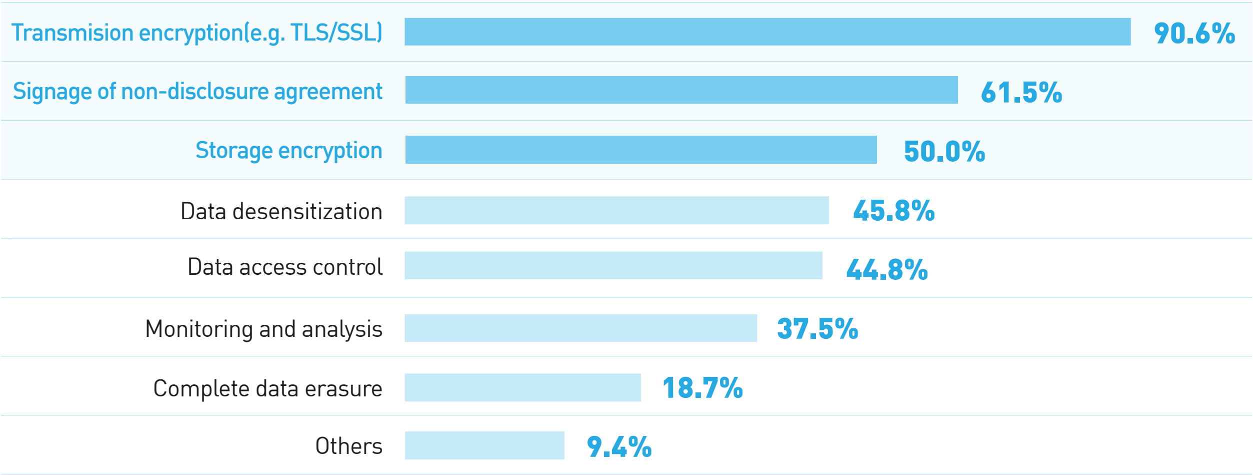
The top 3 data types that will be used in deployed or soon to be deployed Cloud service in FSI China are product information, customer data and IT services data. The data types that will be given the least priorities are salary and financial datas.

Data Protection and Privacy Concerns in Cloud



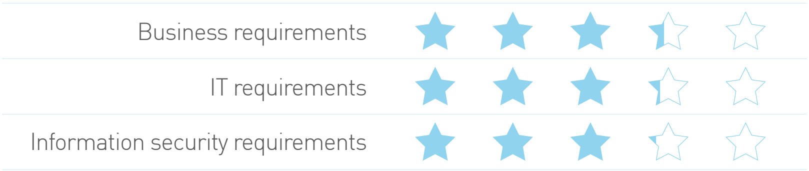
Out of all the data protection and privacy concerns that are listed in the survey, although results do not show a huge difference in scores among the options, malicious attack or data stealing, data confidentiality and lack of data control (lack of governance) are the top 3 concerns in Cloud in FSI China.

Protecting Data in Transit/At Rest for Cloud Applications



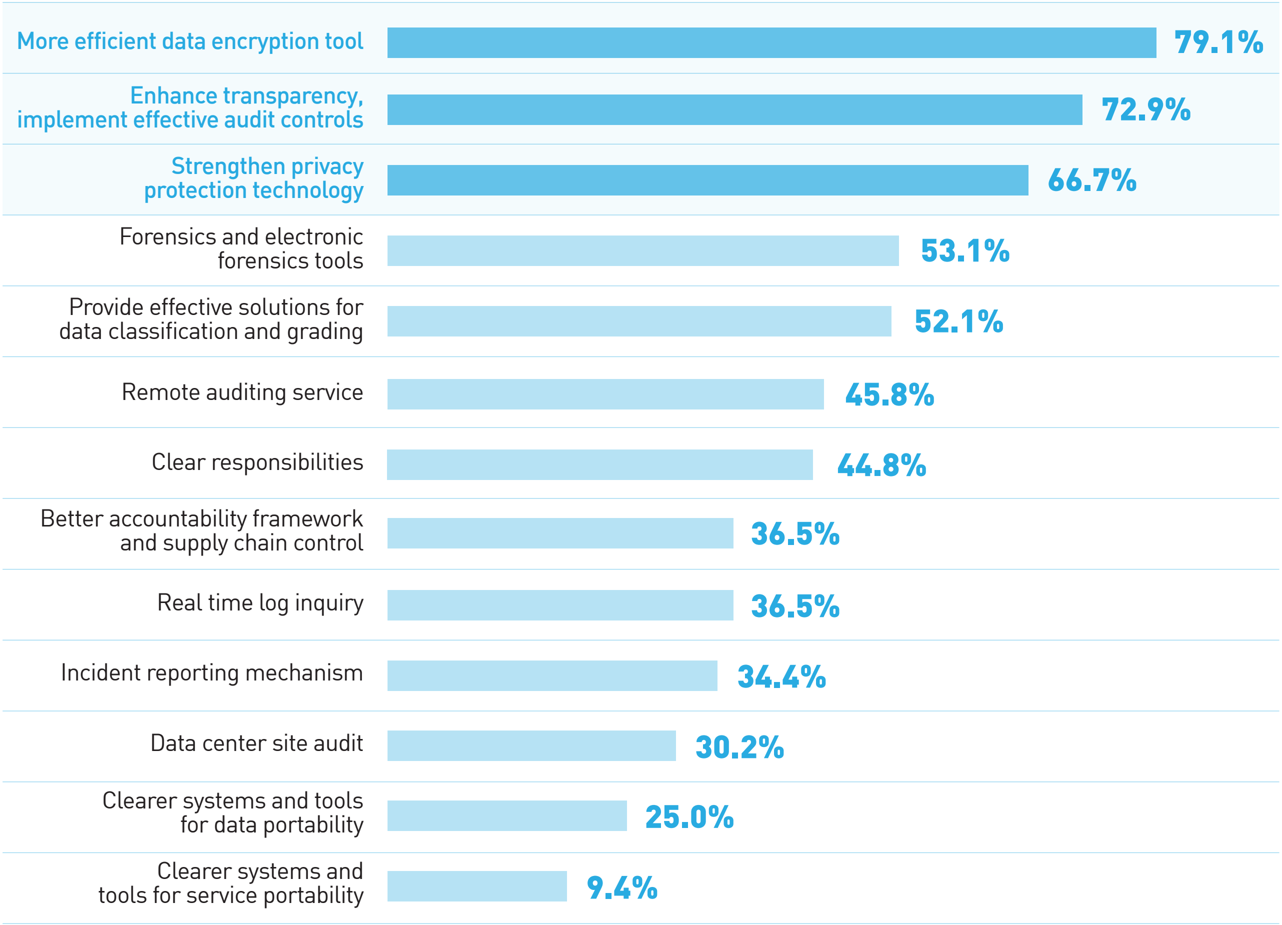
Most FSIs address data in transit and data at rest for their Cloud applications by transmission encryption (e.g.TLS/SSL). Other popular methods include signing of non-disclosure agreement, storage encryption, data desensitization and data access control.

Cloud Service Provider Satisfaction Rating



Figures show that FSIs in China are most satisfied with their Cloud service provider in terms of business requirements, followed by IT requirements and lastly information security requirements.

Functions/Services of Interest



The top 3 functions or services that FSIs will like Cloud service providers to provide are enhancing transparency, implementing effective audit controls, providing a more efficient data encryption tool, and strengthening privacy protection technology. Comparatively, other functions such as incident reporting mechanism and remote auditing service are less desirable.

Top 10 Concerns While Selecting a Cloud Service Provider

Reliability (high availability and minimize the impact on business)	★★★★☆
Safety (hold authoritative security certification and an auditable overall management and control)	★★★★☆
Compatibility (associativity with mainstream applications and systems)	★★★★☆
Service (accurate, fast, focus on meeting customers' requirements)	★★★★☆
Flexibility (modify product in a timely manner to fulfil customer requirements)	★★★★☆
Credibility (trusted brand and good reputation in the market)	★★★★☆
Transparency (clear billing table and detailed financial report)	★★★★☆
Function (simple, easy to understand the characteristics and processes of products)	★★★⯪☆
Stability (strong capital investment and good profit growth trend)	★★★⯪☆
Price (deployment and operating costs are lower than other similar services)	★★★⯪☆

Reliability, safety and compatibility are the top 3 concerns that FSIs have when they are selecting a Cloud service provider. Price is apparently the least concerned factor of all.

Standards/Certifications

Administrative Measures for the Graded Protection of Information Security - Ministry of Public Security	★★★⯪☆
Trusted Cloud Service Assessment - Ministry of Industry and Information Technology	★★★⯪☆
GB/T 220800, ISO 27001 - CNAS/UKAS	★★★☆☆
CSA STAR Certification - Cloud Security Alliance	★★★☆☆
WebTrust, SysTrust - AICPA & CICA	★★⯪☆☆
ISO 22301 - UKAS	★★⯪☆☆
SOC SSAE 16 - AICPA	★★⯪☆☆
Service governance effectiveness certification report - AICPA & CICA	★★⯪☆☆

Majority of the FSIs are looking at Chinese Standards such as the Trusted Cloud Service Assessment by the Chinese Ministry of Industry and Information Technology, the Administrative Measures for the Graded Protection of Information Security by the Chinese Ministry of Public Security and GB/T 220800:2008-2013 Information Security Management System Requirements and International Standards such as ISO 27001:2005/2013 and CSA STAR Certification. Service Organization Control Reporting, WebTrust and SysTrust by AICPA/CICA, ISO 22301 and the SOC SSAE 16 Reporting Standard are standards/certifications that the Chinese FSIs are paying less attention to.

2.4. Other

Top Cloud Adoption Requirements

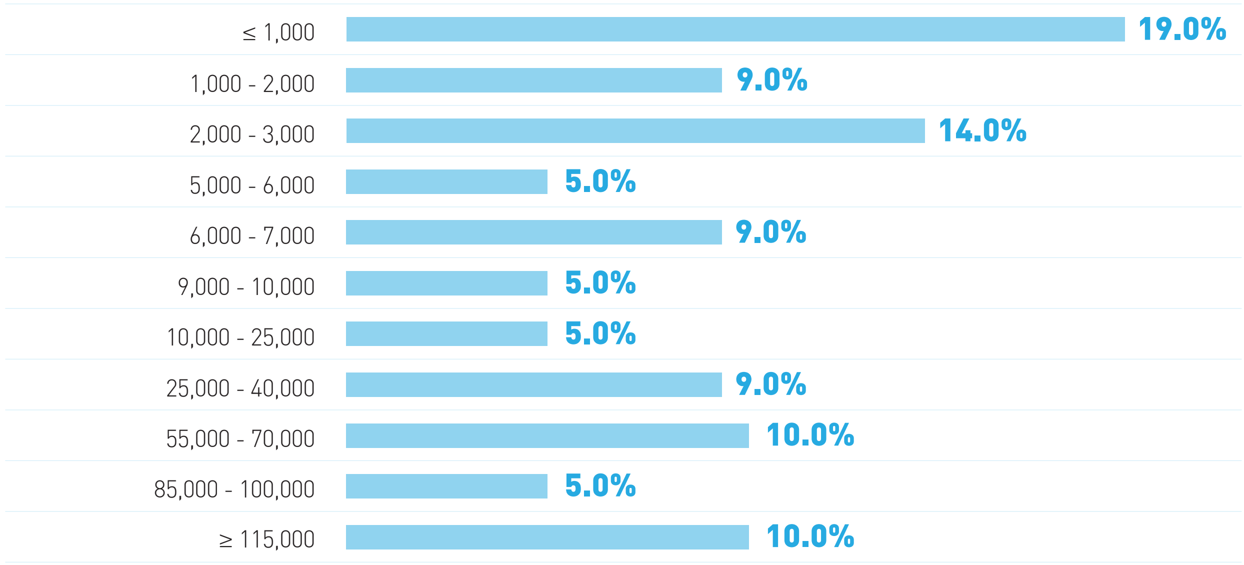
Overall Cloud computing planning and implementation	★★★⯪☆
Risk assessment and continous risk management against Cloud provider	★★★☆☆
Migration and implementation of existing system	★★★☆☆
Select the most suitable Cloud service provider according to the characteristics and needs of my organization	★★★☆☆
Operation management against Cloud provider	★★★☆☆

Overall Cloud computing planning and implementation is the key factor that the FSIs require when they are adopting Cloud. Risk assessment and continuous risk management against Cloud provider, and migration and implementation of existing system are the 2 other top requirements by the FSI industry in China.

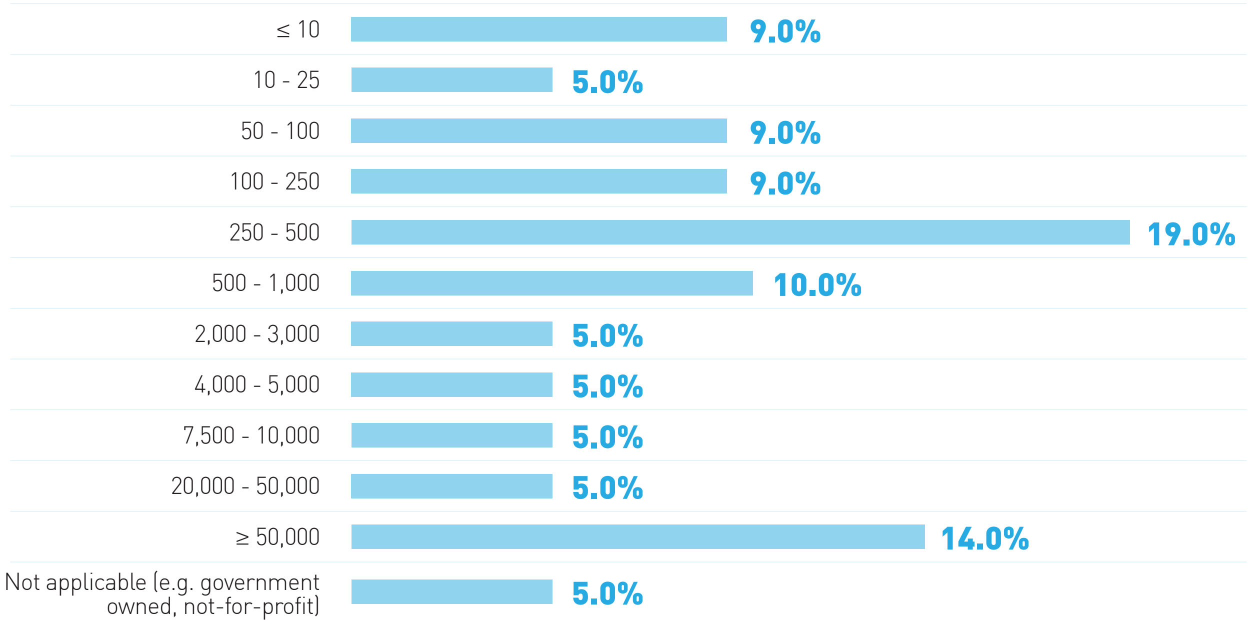
3. Methodology

The survey was conducted through a questionnaire methodology for a period of 3 months. The survey was originally sent to individuals from the CSA Chinese community and participants from EY.

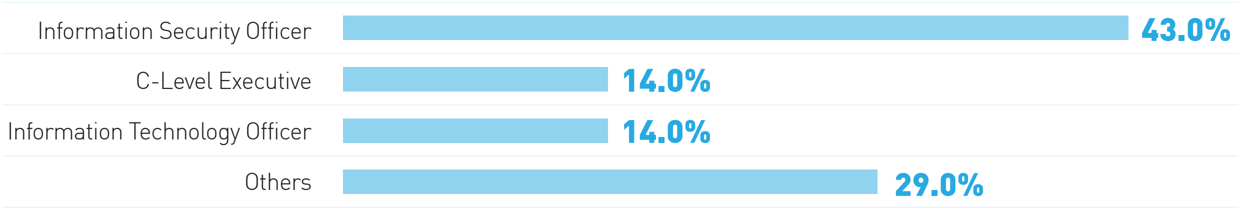
Organization Scale



Average Annual Revenue in the Past 3 Years (in CNY)



Designation



About Cloud Security Alliance

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.