



## BSA SUBMISSION - TRAI CONSULTATION PAPER ON CLOUD COMPUTING

July 25, 2016

Shri A. Robert J. Ravi,  
Advisor (QoS)  
Telecom Regulatory Authority of India  
Mahanahgar Door Sanchar Bhawan  
Jawahar Lal Nehru Marg (Old Minto Road)  
New Delhi – 110012

Dear Sir,

**Subject: Response to the TRAI Consultation Paper on Cloud Computing**

This is with reference to the TRAI Consultation Paper on Cloud Computing issued on 10<sup>th</sup> June, 2016.

In this regard, please find enclosed the following:

1. Submission from BSA | The Software Alliance (“BSA”) on the Consultation Paper [Annexure 1]
2. BSA’s 2016 Global Cloud Computing Scorecard with the India country report [Annexure 2 and 3]

We hope our submission and our cloud computing report are useful to the consultation process and will merit your kind consideration. We look forward to participating in this important discussion and stand ready to answer any questions you may have.

Thanking you,

Yours Sincerely,

---

Jared Ragland, Ph.D.  
Senior Director, Policy  
Asia Pacific

## Annexure I

### BSA's Submission to the Consultation Paper on Cloud Computing

#### Introduction

BSA | The Software Alliance ("BSA")<sup>1</sup> is thankful for the opportunity to offer comments on the Consultation Paper on Cloud Computing ("Consultation Paper") released on June 10, 2016.

As the leading advocate for the global software industry, BSA is greatly interested in contributing to initiatives that seek to advance cloud computing. We commend the efforts of the Telecom Regulatory Authority of India (TRAI) to conduct this Consultation.

The software industry is undergoing a dramatic transformation. BSA members increasingly provide a wide array of Internet-enabled services, such as cloud computing services, data analytics, security solutions, and much more. This is in addition to a full range of software solutions that are more often downloaded online or used on remote servers. These technologies collapse distance as never before, allowing companies to operate seamlessly in international markets — interacting with suppliers and serving customers wherever they may be. This is the new, digitally-enabled face of trade.

We believe that a policy environment that enables businesses, consumers and governments to leverage the full benefits of cloud computing is the key to driving the digital economy. We observe that the countries with the most favorable policies for cloud computing are those which prioritize free movement of data across borders, respect for international standards, protection of privacy and intellectual property, and robust enforcement and deterrence of cybercrime. We also find that many countries recognize that coordination of national cloud computing policies, both internally and with those of other nations, will facilitate benefits for all countries participating in the global economy.

Cloud computing remains in a relatively early stage of development. In some areas, limited government regulations are appropriate, for example to establish data privacy frameworks or provide for consumer protection. In such cases, it is important for the Government of India to keep such regulations in line with emerging international trends and best practices. For many of the issues raised in this Consultation Paper, an overly-regulated approach is likely to inhibit development, deployment and growth of cloud computing services, to the detriment of Indian businesses and other entities.

Despite cloud computing's early stage of growth, various standards bodies have, over the past decade, made significant efforts and progress in developing industry standards and best practices. Therefore, as the Government of India seeks to establish an enabling policy environment to promote cloud

---

<sup>1</sup> BSA | The Software Alliance ([www.bsa.org](http://www.bsa.org)) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

computing, we urge TRAI and other relevant agencies to work together and, where possible, look to industry best practices rather than formal regulations.

Procurement is a related and extremely relevant aspect for the development of cloud computing. Traditional purchasing practices and contract terms may hinder the scalable, cost-effective, and innovative nature of cloud computing. Quick and flexible procurement processes that are not hampered by burdensome terms and conditions will allow users to fully leverage the vast array of benefits offered by cloud computing technologies.

As the Government of India develops and implements policies to foster the adoption of cloud computing, it is paramount that TRAI and other Indian government agencies take a coordinated approach and provide clear and predictable indications to the market on the policies to be adopted and the objectives such policies seek to achieve. As TRAI has done with this Consultation Paper, it is also critical that the Government of India continue to seek the input of interested and relevant private sector stakeholders to inform policy making in this area. This will allow investors to plan and execute long term strategies and investments in the Indian market and will help ensure that India is positioned to become a global leader in developing an effective, trusted, transparent and restrained regulatory environment, that works well with emerging international practices, and allows Indian businesses and consumers to fully benefit from existing and future opportunities presented by cloud computing and related services.

Indeed, the stakes are very high for India given the large and increasingly cloud dependent domestic information technology (IT) and business processing management (BPM) industries. According to the industry group NASSCOM, the Indian IT-BPM market in 2016 is over USD \$143 billion, with exports exceeding USD \$100 billion.<sup>2</sup> Any measures adopted that slow the growth of cloud computing globally and within India could put at risk the growth of this important industry in addition to the many other costs to the Indian economy.

BSA and its members have extensive experience working with governments and other stakeholders around the world on policies that promote cloud computing. We share these views hoping to assist TRAI in its efforts to map out the necessary policies that will help promote increased development, deployment and adoption of cloud computing in India.

### **BSA Global Cloud Computing Scorecard**

BSA, and our research partner Galexia, have been conducting a survey of major cloud computing markets since our first Global Cloud Computing Scorecard was released in 2012.<sup>3</sup> We recently published our third and the most recent and updated study, the 2016 Global Cloud Computing Scorecard,<sup>4</sup> earlier this year in April. In these studies, BSA ranks the countries surveyed according to their cloud computing readiness.

---

<sup>2</sup> NASSCOM IT-BPM Snapshot at <http://www.nasscom.in/indian-itbpo-industry>.

<sup>3</sup> The 2012 and 2013 BSA Global Cloud Computing Scorecards and accompanying country reports can be found at <http://cloudscorecard.bsa.org/2012/> and <http://cloudscorecard.bsa.org/2013/> respectively.

<sup>4</sup> 2016 BSA Global Cloud Computing Scorecard and accompanying country reports at <http://cloudscorecard.bsa.org/2016/>.

Each country is graded on its strengths and weaknesses in seven key policy areas, encompassing the laws, regulations and IT infrastructure necessary for the support and growth of digital technology and cloud computing. These areas are: 1) data privacy; 2) security; 3) cybercrime; 4) intellectual property rights; 5) standards that enable data portability and international harmonization of rules; 6) promotion of free trade; and 7) IT readiness and broadband deployment.

India's relative ranking within this group of 24 countries has remained relatively stable over the last 5 years, coming in 19<sup>th</sup> (2012), 17<sup>th</sup> (2013), and 18<sup>th</sup> (2016) out of 24 countries surveyed even though India's absolute score has steadily climbed, from 50/100 (2012) to 53.1/100 (2013) to 56.1/100 (2016), indicating improvements in cloud computing readiness over time. That said, given that some other countries have progressed even faster, India risks falling farther behind in its global competitiveness. India can and must foster a conducive policy and regulatory regime for cloud services to flourish and avoid imposing onerous and burdensome obligations that can impede the adoption and provision of cloud computing.

For more information, the BSA 2016 Cloud Computing Scorecard and accompanying India Country Report are attached to this submission as Annexures II and III, respectively.

### **BSA's Response to Questions in the Consultation Paper**

Because BSA is an industry association representing many of the leading global cloud computing service providers (CSPs), we have attempted to focus our responses on those questions amenable to industry wide input. We have chosen not to answer all of the questions in the consultation, especially where we felt questions were specific to individual company practices or experiences and not suitable to an industry wide response.

### **Financial & Operational Benefits**

*Question 1. What are the paradigms of cost benefit analysis especially in terms of:*

- a. accelerating the design and roll out of services*
- b. Promotion of social networking, participative governance and e-commerce.*
- c. Expansion of new services.*
- d. Any other items or technologies. Please support your views with relevant data.*

A range of factors must be considered to conduct a cost-benefit analysis and evaluate various cloud computing technologies. The Consultation Paper highlights capital expenditure cost savings as a primary benefit, and describes security, reliability, interoperability and vendor lock-in as threats from using cloud services.

It also emphasizes how cloud computing offers greater efficiency, scalability, dynamism, reliability and availability that would yield better security, more innovation and lower barriers of entry for small- and medium-sized enterprises (SMEs).

Companies and government agencies should consider how cloud computing services can **accelerate the design and roll out of services** by enhancing IT system efficiencies and the savings of reduced on-premises IT costs. Such entities must adapt to variable cost procurement models that incorporate pay-per-use approaches that allow for faster and more tailored services, and move away from fixed capital expenditure procurement models. Cloud services, by their nature, can offer real-time scaling which

will improve the agility and dexterity of enterprises and agencies to meet evolving consumer and constituent demands.

The advantages of cloud computing for ***promoting social networking, participative government, and e-commerce*** are both obvious and untapped. Start-ups, e-commerce companies, and government agencies can use the flexibility of cloud computing to quickly provide products and services to customers, to create mechanisms for real-time feedback from customers and constituents, and tailor IT needs to meet rapidly evolving demands and expectations.

Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) models allow enterprises and agencies to ***expand new services*** quickly by creating a rapidly adjustable development and deployment environment for new services.

### Competitive Market for CSPs

By their very nature, cloud technologies operate across national boundaries. The cloud's ability to promote economic growth depends on a global market that transcends barriers to international trade and data transfers, such as preferences for particular products or providers and data or hardware localization requirements.

In order for the benefits of adopting cloud computing to emerge, the Government of India should focus on creating a competitive market for cloud computing services. This will include avoiding unnecessary regulatory burdens, promoting innovation and adhering to internationally recognized standards.

The Government of India should not adopt policies that are intended to create advantages for Indian cloud providers operating in India to the detriment of foreign providers. Rules that protect providers that operate in India, shielding them from healthy international competition, will tend to freeze innovation, raise production costs, and make Indian CSPs less competitive in the global market that their cloud services can serve.

*Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organisation?*

### Advantages of Cloud Computing

Cloud computing is a term that includes IT infrastructure, processing, storage, networks, operating systems, and applications that are available on demand in variable quantities. A cloud-based business model enables companies to have stronger budget control and greater agility in accessing the technology they need.

Service requests in the cloud environment are highly automated, allowing consumers to acquire, utilize and adjust services rapidly with little cost to the enterprise or agency. The end-user of cloud service is only billed for the services utilized, which allows more efficient use of limited resources, and to adapt to changes in expected IT usage.

The gap between expected and actual usage combined with large up front capital expenditures, can be a large burden, especially on smaller enterprises and agencies. Small companies may have difficulty raising the necessary capital to invest in technology. Moving from a CapEx to OpEx model removes

such limitations by allowing smaller projects to be undertaken without incurring large sunk costs from unnecessary capital investments.

The move to the cloud and capitalization on its benefits across the board is hardly inevitable, and an urgent task lies ahead for governments. In order for societies to obtain the benefits of the cloud, policymakers must provide a legal and regulatory framework that will promote innovation, provide incentives to build the infrastructure to support it, and promote confidence that using the cloud will bring the anticipated benefits without sacrificing expectations of privacy, security, and safety.

We believe that there are significant economic benefits to be gained from a move to cloud computing accruing directly through reduced costs and indirectly by allowing for increased focus on core business functions. Many organizations still operate networks that are decades old. Gradually, these networks have been enhanced to support new services, but their basic architecture has not changed. These dated networks are costly, prone to failure and difficult to manage. As just one pertinent example, a large, dated on-premises IT system costs significantly more in electricity and maintenance as a function of capability than newer cloud-enabling data centers. Overall, cloud computing gives organizations the ability to add business value through renewed focus on core activities.

Cloud computing is also very beneficial when organizations need to deploy capacity to handle their peak demands. Since a CSP can reallocate resources across many enterprises with different peak periods, the CSP needs to deploy less total capacity to handle the same amount of business operations and services. Average unit costs are reduced by distributing fixed costs over more units of output. Larger cloud providers can therefore achieve significant economies of scale.

Among the biggest beneficiaries of cloud computing are SMEs. Cloud computing allows SMEs to leverage enterprise grade IT tools to which they would not otherwise have affordable access. Utilizing cloud computing, SMEs are able to scale IT use rapidly. Excessive regulation tends to disproportionately impact SMEs as costs, including for licensing, compliance, and related issues, go up and the cost-benefit ratio is undermined. India should, therefore, avoid over-regulation that could negatively impact the development of cloud computing.

In addition to the cost-benefits highlighted above, cloud computing services offer significant security benefits. CSPs can provide a level of protection for their customers' digital assets that exceeds what most individual companies are capable of providing on their own. This is particularly important for SMEs. The security benefits provided by the use of cloud services include but are not limited to: 1) increased physical security, as access to cloud servers is restricted to authorized personnel only, constantly monitored, and protected through technologies such as multifactor authentication; 2) regular security audits and assessments to detect and deter security incidents; and 3) data loss mitigation in the event of natural disaster or power outage through the use of backups located in various geographic locations.

## **Cloud Service Models**

*Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?*

There are many factors that enterprises and agencies should consider when selecting the type of cloud service deployment model. All enterprises should be concerned with the effectiveness and security of the service, and the trustworthiness of the provider. Smaller organizations are likely to be drawn to public cloud offerings because of ease of use and cost considerations. Larger organizations may look to CSPs that provide multi-tenant or public cloud deployments that meet larger organizations' regulatory needs and exceed their operational requirements and security considerations. Many CSPs are able to demonstrate security and privacy commitments sufficient to demonstrate their compliance with numerous regulatory regimes and other industry and government established assessment tools. CSPs can offer operational flexibility in IaaS and PaaS solutions, relatively low maintenance in SaaS solutions, and security at scale, including as a result of their visibility into malware and their ability to retain best-in-class security professionals.

A major advantage of adopting cloud solutions for enterprises and agencies of all sizes is that leading CSPs are often much more capable of providing high quality IT services, 24/7 support, and risk management solutions than in-house IT resources. This is especially true for SMEs that have limited expertise with the ability to effectively manage IT costs, security and regulatory compliance.

### **Cloud Security in relation to Data Migration**

*Question 4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?*

CSPs tend to facilitate migration and portability in creative and innovative ways without regulatory intervention because every cloud vendor has a business interest to attract customers from their competitors and will make available tools to facilitate migration. In addition, for some SaaS services where no data resides with the cloud service provider, migration is as easy as rerouting traffic from one gateway to another.

Rather than attempting to "prescribe a secure migration path", governments should encourage the adoption of voluntary, transparently developed, industry-led international standards, while also working to minimize conflicting legal obligations on CSPs.

The specific mechanisms for transferring data from legacy systems to CSPs and from one CSP to another will depend heavily on the specifics of each organization and their existing data structures. BSA members offering cloud computing services have developed a variety of solutions that can be tailored to their customer for secure transfer of data from one system to another. In some cases, this may be rather straightforward. In others, it may be more difficult, such as when the data is tightly associated with particular applications and is not easily convertible to alternative systems.

As CSPs continue to evolve, it is likely additional voluntary international standards will emerge, and governments should support industry-led efforts to promote data portability. However, a prescriptive regulatory approach to address cloud migration is likely to be counter-productive and would likely limit the services available in the market place without improving data migration capabilities.

*Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?*

As cloud computing solutions evolve and mature, industry standards are developing for security, interoperability, and data portability. Because the ease or difficulty of migrating data from on-premises systems to CSPs, or one CSP to another, varies greatly depending on the kinds of data and data uses involved, it is critical that governments avoid prescriptive, one-size-fits-all requirements.

Governments should remain technology neutral and avoid imposing any limitations on, or preferences for, particular business models and licensing models. Open source and proprietary technologies are increasingly integrated into the same services and software solutions and each model has its respective advantages and disadvantages. The Government of India should establish policies that ensure that business, government agencies and consumers have the freedom of choice to determine and select which combinations of products and services will provide the best value for money given the particular enterprise needs. The role of government should be to encourage the use and adoption of standards that are global, voluntary, and developed through industry-led multi-stakeholder processes which reduce costs, promote innovation, and facilitate interoperability through open and transparent processes.

Internationally, much work has been done in various industry bodies to set standards or processes for promoting interoperability. Since cloud computing, by its nature, works across international borders to achieve economies of scale, enhanced reliability and security, the best way to ensure interoperability is, therefore, to adhere to the work already done by following industry best practices and, where they have been widely adopted, international standards.

BSA members adopt and comply with a variety of standards, and governments should avoid “picking winners” from among different standards. The government should participate in standards setting activities as a convener, as a trusted expert, and as a major purchaser of technology and implementer of standards. Finally, the government should rely on voluntary, consensus based, industry driven standards instead of setting technical requirements themselves.

We recommend the Government of India: (1) support IT industry organizations developing international standards that will ensure optimal portability and interoperability; (2) accept and utilize widely adopted international standards and certifications; and (3) refrain from requiring use of local standards and certifications.

*Question 12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?*

As stated before, we urge against a prescriptive regulatory approach for data portability. The provisions necessary will vary and depend on the kinds of data and enterprises involved. Some BSA members have established protocols, including strong encryption of data in transit, to ensure secure data transfers and to minimize security risks. Some of our members also offer ready solutions for data exportation into various standard data formats for users that wish to migrate their data to alternative IT systems or CSPs. The details will be determined by the nature of the service provided, the needs of the end-user, the kinds of data involved and their various uses, as well as many other factors. The specific terms of data exportation should be clearly laid out in the contract between the end-user and the CSP and not through regulation.



Rather than attempting to regulate in this area, or impose prescriptive rules, we urge governments to support emerging international standards to promote security, interoperability and data portability, and to avoid imposing additional country-specific certification requirements that only raise costs for the CSPs and end-users without improving data portability.

## **Data Ownership**

*Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?*

Contractual provisions are the appropriate mechanism for regulating the rights and obligations of end-users and CSPs in the cloud environment. Governments should avoid establishing specific requirements for how consumers control their data, as they are likely to inhibit growth and innovation in cloud computing services and limit consumers' choices of available CSPs. Instead, governments should promote policies that advance the goal of transparency so purchasers of cloud-based services can make informed decisions.

Data protection and privacy laws and regulations are designed to provide protection of personal data. The Government of India should seek to align data protection regimes with internationally accepted models so that they will ensure continued international data transfers, which are the lifeblood of cloud computing services.

## **Cloud Security**

*Question 10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.*

BSA member companies have a deep and long-standing commitment to protecting consumers' data across technologies and business models. Consumers will only take advantage of the benefits of new technologies, such as cloud computing services, if they trust that the data they entrust to a CSP will be secure, protected and not used in unexpected ways. BSA member companies offering cloud services provide enhanced solutions both by adopting, developing and implementing advanced security solutions, and in some cases providing Security-as-a-Service solutions, directly to both end-users and to other CSPs.

It is critical that CSPs are able to adopt and implement cutting-edge cybersecurity solutions that can be adapted and tailored to the different needs of different users and use cases. Governments should avoid imposing any requirements to use particular technologies or services. Instead, national cybersecurity frameworks should be risk-based and prioritized, technology neutral, practicable, flexible and respectful of privacy and civil liberties.<sup>5</sup>

When considering the security implications of cloud computing, it is important for the Government of India not to make inaccurate assumptions about the security of cloud services versus traditional, or "on-premises" IT systems. An on-premises system that is networked and connected to the Internet can be at as much risk or more as data or processes stored in the cloud. In fact, security may be more effectively managed by a sophisticated and experienced cloud provider than by in-house IT

---

<sup>5</sup> Asia-Pacific Cybersecurity Dashboard at <http://cybersecurity.bsa.org/2015/apac/>

departments. This is especially true for small organizations and agencies, and SMEs. The alternative of keeping data and processes offline can exacerbate availability and reliability concerns and undermines the real and potential benefits of effectively utilizing IT systems in business operations.

There are a variety of steps that many CSPs take to enhance the security of their systems. These often begin with physical security. Facilities are secured and monitored and access of personnel is controlled. Data can be secured in a variety of ways, including with strong encryption, both at rest and in transit. At the operational level, CSPs may choose to comply with a variety of security-related standards and certifications. Many will submit to third party audits or other validation measures to assure private- and public-sector customers that the security measures in place are effective. Leading global standards related to information security demonstrate a provider's security commitments across the relevant domains. Governments can achieve high security outcomes by either using those standards or mapping their own security requirements to their controls, minimizing the differences or novel requirements as much as possible to ensure efficiency and reduce costs.

Like with interoperability and portability, governments should promote the development and adoption of voluntary, transparently developed, industry-led international standards, and recognize certifications from internationally accredited entities. Unfortunately, the Government of India imposes local security testing requirements in addition to international testing requirements. These requirements increase costs, which can lead to reduced security as end-users may have less access to cutting-edge security solutions available on the global market.

The perpetrators of cyber-attacks are constantly adjusting their methods, targets and technologies. The imposition of highly prescriptive security rules must be avoided as they fail to recognize new and evolving methods and technologies which could, in turn, limit the ability of CSPs and others to anticipate and respond to emerging threats.

### Encryption Policy

India lacks a uniform, consistent and effective encryption policy. Most other countries allow the use of strong encryption standards ranging from 128-bit to 256-bit to ensure the security of sensitive information exchanged via the Internet and other networks. In India, however, only 40-bit encryption can be used without additional regulatory approval according to the Department of Telecommunications' Guidelines for the Grant of License for Operating Internet Service (ISP Guidelines).

Encryption standards differ greatly from one regulatory agency to another in India, each having their own specific standards. In September 2015, the Government of India published a Draft National Encryption Policy that was withdrawn shortly after publication. The draft raised a number of concerns including restrictions on the use of commercially available encryption (by restricting key lengths for example) and mandates to disclose proprietary information.

We urge the Government of India to fully consult with relevant stakeholders before developing or implementing a National Encryption Policy. The Government of India should adopt a clear policy permitting the use of strong-encryption. The Government of India should also avoid any efforts to require technical access solutions (e.g. backdoors) or encryption-key escrow systems, for any such

efforts will only weaken vital data security for all. As we report in a recent publication on encryption,<sup>6</sup> “Cryptographers warn that it is impossible to weaken encryption without strengthening the hands of hackers and foreign adversaries.”<sup>7</sup>

## **Obligations on CSPs**

*Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider(CSP); and (b) End users?*

In a cloud environment, responsibilities are often shared between the customer and the cloud service provider (CSP) depending on the business model.

The responsibilities for managing risks will vary depending on the cloud delivery model. For example, end-users have less control over risks in SaaS models compared to IaaS models. In the latter, the user may be responsible for ensuring that the operating system is patched for security vulnerabilities, while in the former, the operating system is not exposed to the end user. Given the variety of cloud models and CSP/end-user arrangements, it is neither reasonable nor realistic for the government to effectively mandate outcomes across these various models. Instead, the roles and responsibilities of CSPs and their customers/end-users should be decided between the parties in their agreements.

## **Cross-Border Data Flows**

*Question 14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?*

The ability to transfer data internationally is the lifeblood of cloud computing and the modern digital economy. The success of cloud computing depends on users’ trust that their information will be properly protected. At the same time, to maximize the benefits of the cloud, including the resilience that results from dynamic geographical redundancy, CSPs benefit from being able to move data through the cloud in the most efficient way. Cross-border data flows enable international commerce and are also critical for:

**Systems Integrity:** Global cloud and other Internet-enabled service providers invest in state of the art security and reliability. Limiting cross-border data transfers will reduce the ability of cloud customers from utilizing CPS with the strongest security and reliability features.

**Redundancy and Reliability:** Cloud and other Internet-enabled service providers often store data in geographically dispersed locations, making it harder for hackers to gain access and ensuring that if natural disasters or other unforeseeable forces damage or disable one data center, customer data is not lost and end-user services are not disrupted.

**Efficiency – Data Transmission:** Internet-enabled data transfer relies on the efficient transfer of data from one point to another to maximize transmission speed. The nature of the Internet is such that

---

<sup>6</sup> Encryption: Securing Our Data, Securing Our Lives, found at <http://encryption.bsa.org/>

<sup>7</sup> [http://encryption.bsa.org/downloads/BSA\\_encryption\\_primer.pdf](http://encryption.bsa.org/downloads/BSA_encryption_primer.pdf) - page 10.

often the fastest and most efficient route for data transfer from one location to another is not a straight line but through geographically dispersed connection points and servers.

Efficiency – Data Processing: The cost of processing data often depends on the operational demands on particular servers and data centers. The ability to transfer data to underused equipment, for example during off-peak hours, minimizes the costs of processing.

BSA members invest significant efforts to ensure that their customers' sensitive information is used appropriately and fully protected wherever it is transferred, stored or processed.

As the policies to promote the adoption of cloud computing are further developed, the Government of India should ensure that data protection and cybersecurity frameworks are in place while: 1) avoiding all unnecessary restrictions on cross-border data flows; and 2) recognizing the need for service providers to determine where infrastructure is located to maximize efficiencies of scale and economy and to ensure the most secure and reliable services.

Members of BSA have a deep and long-standing commitment to protecting consumers' data across technologies and business models as they recognize that consumers are only comfortable taking advantage of the benefits of new technologies, including cloud computing, if they trust that their information is protected.

The adoption of an accountability model, as established by the OECD, which requires organizations that collect data to be responsible for its protection no matter where or by whom it is processed would appropriately protect users. This approach requires organizations transferring data to take appropriate steps to ensure that any obligations – in law, guidance or commitments made in privacy policies – will be met.

In sum, governments should avoid all unnecessary mandates regarding the location of data storage and the restriction of international data transfers, as these policies reduce the efficiency and efficacy of cloud services and unnecessarily limit consumer choice.

## **Lawful Interception**

*Question 15. What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?*

Governments should leverage existing mutual legal assistance treaty (MLAT) arrangements and coordination via INTERPOL to address lawful interception requirements beyond national boundaries. To enhance lawful access to information, the Government of India should enter into MLATs with more international partners. For countries with which India has already signed an MLAT, it should focus on resolving interpretational differences and enhancing the efficiency of the processes in both directions.

Access requests should only be valid when backed by proper legal authorization. Any obligation imposed on a CSP to decrypt or provide access to data should apply only if the system architecture enables the decryption to take place (e.g. where the vendor or operator holds the key). It should not be required if the architecture does not allow the vendor or operator to perform decryption of the

requested data. Encryption used by corporate enterprises intended to create a secure private network for corporate communications and should not be subject to requests for access to unencrypted data.

## **Licensing & Registration**

*Question 16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud service providers so as to subject them to the obligations thereunder? Please comment with justification.*

As mentioned above, cloud computing remains in a relatively early stage of development. What is described as cloud computing today is likely only a small subset of the cloud computing services that will be available in the future. It would be very counterproductive to attempt to define the scope of cloud computing in law, as this could chill innovation and set unnecessary boundaries on the evolution of cloud services.

Therefore, BSA opposes efforts to impose any sort of licensing framework on cloud service providers (CSPs), now or in the future. Cloud services are provided over telecom infrastructure which is already licensed and regulated. Therefore, there is no need for any additional licensing or regulatory oversight by TRAI on cloud services per se.

Any additional compliance requirement like licensing or registration would go against the Administration's spirit of liberalization and "ease of doing business" objectives.

## **Jurisdictional Issues**

*Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?*

This question suggests that TRAI may be considering a separate or additional protocol for CSPs with respect to lawful access. On the contrary, the same framework that applies to existing Internet services should apply to CSPs. The issue of territorial jurisdiction does not differ between cloud data and other forms of digitized information available on the Internet.

Furthermore, CSPs do not necessarily "own" the data. Nor are they necessarily authorized to access the data, or monitor it. CSPs cannot police the content and conduct of users on self-service platforms and should not be held responsible for the content of the information stored on processed on their services.

As discussed above, access requests should only be valid when backed by proper legal authorization.

## **Government Cloud**

*Question 18. What are the steps that can be taken by the government for:  
a. promoting cloud computing in e-governance projects.*

India should consider implementing the Meghraj "Cloud First Policy" more broadly. India should develop a document which sets out general guiding principles for a "cloud first" approach for

government ministries and agencies to consider in adopting cloud computing solutions as a primary part of their information technology planning and procurement. All government-led, government-controlled programmes should be mandated to go “cloud first”.

Another way to increase public sector adoption of cloud is for a central government agency to develop shared services for public sector customers, making specific services available to all government agencies. These could also be extended to the private sector such as SMEs to increase their adoption of cloud services.

#### *b. promoting establishment of data centres in India.*

The Government of India should establish incentives for investing in data centers in India, but should avoid mandates. Many CSPs that do choose to invest in data centers in India are likely to be interested in serving the regional market place. If countries adopt requirements for locate servers in their markets in order to offer services, such as cloud computing services, this will fundamentally interfere with the economies of scale and rational distribution of infrastructure that underpins the potential of these services to drive productivity and economic growth. There may be a variety of incentive schemes that the Government of India might consider, but a key factor will be to ensure that the basic infrastructure (reliability of power, transportation, internal and international bandwidth) is competitive with other global markets.

*Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?*

There is no necessity for a dedicated cloud for government applications, unless there is a very clear reason for it. In fact, a dedicated cloud for government applications negates a number of cost-benefits of cloud computing’s shared resource model where the cloud service provider owns and maintains the network connected hardware required for their cloud services.

A dedicated cloud need not be considered, unless (1) there are specific security requirements which an outsourced cloud vendor is unable to fulfill, or (2) there are technical requirements which an outsourced cloud provider is unable to fulfill.

A separate government cloud does not increase security, either in a single-tenant or multi-tenant environment. Instead, government agencies should decide what kind of architecture they need in order to meet their needs and achieve their objectives.

#### **Data Centre Infrastructure**

*Question 20. What infrastructure challenges does India face towards development and deployment of state data centres in India? What should be the protocol for information sharing between states and between state and central?*

According to the 2016 BSA Global Cloud Computing Scorecard, India is struggling with IT readiness and broadband deployment compared to other countries. Much of this relates to demographic and other factors beyond IT policies. That said, it is clear that India should aggressively adopt policies that will provide incentives for private sector investment in broadband deployment and that will promote universal access to broadband connectivity.

Without the basic infrastructure in place, it will remain difficult to distribute the benefits of enhanced cloud computing to the economy as a whole. For example, while progress has been made in the electricity and sustainable power development in India, challenges in this area still remain due to the lack of a cross-country electrical grid.



# 2016 BSA GLOBAL CLOUD COMPUTING SCORECARD

Confronting New Challenges





# CONTENTS

- EXECUTIVE SUMMARY . . . . . 1
  - BSA Cloud Policy Blueprint . . . . . 3
- KEY FINDINGS . . . . . 5
  - MODERNIZING TRADE RULES: Trans-Pacific Partnership  
Pact Eases Data Sharing . . . . . 6
  - RUSSIA: The Negative Impact of New Data Localization Policies . . . . . 8
- SCORECARD METHODOLOGY . . . . . 13
- USING THE SCORECARD . . . . . 14
- BSA GLOBAL CLOUD COMPUTING COUNTRY CHECKLIST . . . . . 16
- ABOUT BSA . . . . . 24
- ABOUT GALEXIA . . . . . 24



# EXECUTIVE SUMMARY

The 2016 BSA Global Cloud Computing Scorecard — the only report to regularly track change in the international policy landscape for cloud computing — shows that global cloud readiness continues to improve in every region of the world. Even so, important exceptions exist in certain countries that threaten to slow economic growth in those markets.

Information technology (IT) is integral to a nation's economic growth. As a recent IT innovation, cloud computing has added a new dimension to that importance by increasing access to technology that drives economic growth at the national and global levels.

The Scorecard ranks the IT infrastructure and policy environment — or cloud computing readiness — of 24 countries that account for 80 percent of the world's IT markets. Each country is graded on its strengths and weaknesses in seven key policy areas.

The results show progress in some areas, setbacks in others, and the trends that have emerged since the first Scorecard report in 2012. The results also serve as an important roadmap for the future, highlighting the initiatives and policies that countries can — and should — take to ensure that they reap the full suite of economic and growth benefits of cloud computing.

Cloud computing democratizes the use of advanced technologies. Cloud computing allows anyone — a start-up, an individual consumer, a government or a small business — to access technology previously available only to large organizations. These services in return have opened the door to unprecedented connectivity, productivity and competitiveness.

Countries that offer a policy environment in which cloud-computing services can flourish gain in productivity and economic growth. The countries with the most favorable policies are those in which the free movement of data, privacy, intellectual property protections, robust deterrence and enforcement of cybercrime are all important priorities. Many countries also recognize that coordination of national cloud-computing policies with those of other nations will facilitate benefits for all countries participating in the global economy.

But countries inhibiting, or failing to support, the use of cloud computing will not keep pace with those embracing the tool.

This year's results reveal that almost all countries have made significant improvements in their policy environments since 2013. But the stratification between high-, middle- and lower-achieving country groups has widened, with the middle-ranking countries stagnating even as the high achievers continue to refine their policy environments.

The Scorecard can be analyzed in many different ways, but the clearest measurements lie in the scores. The biggest improvers were South Africa (moving up six places), Canada (moving up five places) and Brazil (up more than 4 points but not changing position).

---

**...while many countries are focused on data protection and cybercrime, few are promoting policies of free trade or harmonization of cloud computing policies.**

---

Notably, three of the lowest-ranked countries — Thailand, Brazil and Vietnam — continue to make significant and consistent gains that are closing their gap with next-higher countries. The world's major IT markets remained stable with modest gains.

Negative trends emerged as well. For example, while many countries are focused on data protection and cybercrime, few are promoting policies of free trade or harmonization of cloud computing policies. Russia and China, in particular, have imposed new policies that will hinder cloud computing.

Other countries, such as Korea, may rank among the better-performing markets based on high scores in certain categories but also have adopted restrictive policies that drag down their overall ranking.

Among this Scorecard's findings:

**Data privacy regimes continue to strengthen in most, but not all, countries:**

- ➔ Most countries now have data protection frameworks in place. Canada scored highest based on its comprehensive privacy regime that avoids onerous registration requirements.
- ➔ South Africa received a big boost to its score, moving up six places in rank since 2013, after introducing a comprehensive privacy regime.
- ➔ Russia fell three positions in rank based on its new data protection framework that contains prescriptive data localization requirements. These requirements likely will pose a significant barrier to cloud service providers. Indonesia has also adopted a prescriptive data localization regime.
- ➔ Unfortunately, privacy laws are still absent in several countries. Brazil, Thailand and Turkey have no comprehensive laws in place, while the laws in China, India, Indonesia and Vietnam remain very limited.

**Data security and cybercrime continue to be high priorities for most countries:**

- ➔ Recent high-profile cybersecurity attacks have spurred governments to respond with new cybersecurity laws and policies and most now have legislation to combat the unauthorized access to data in the cloud and cybercrime. A few key jurisdictions continue to have gaps, including China, Russia, Vietnam and Korea.
- ➔ Unfortunately, some countries have been over-prescriptive. China, for example, has imposed an Internet filtering and censorship regime that may act as a barrier to cloud computing.

**Fewer countries are promoting free trade, data portability and the harmonization of standards:**

- ➔ Canada and the United States continue to lead in promoting free trade. A number of countries still provide preferential treatment for domestic suppliers in government procurement or have introduced other barriers to international trade.
- ➔ Damagingly, policies in China, India, Indonesia, Korea and Russia have moved away from accepting international standards and international certifications.

**Obstructive policies continue to keep some countries from advancing:**

- ➔ Despite an improved IT infrastructure score, China dropped four places to next-to-last in the overall rankings due to gaps in privacy protection and cybercrime laws and poor enforcement of intellectual property rights. Other policies discriminate against foreign technology companies and impose onerous certification requirements that hinder free trade. China's extensive regulation of Internet content, including mandatory Internet filtering and censorship, continues to inhibit data movement.



## BSA CLOUD POLICY BLUEPRINT

The economic growth predicted to flow from cloud computing — and the resulting transformation of both businesses and national economies — is predicated on the proper policies being in place in each of the seven areas used in the BSA index:

- **Ensuring privacy:** The success of cloud computing depends on users' faith that their information will not be used or disclosed in unexpected ways. At the same time, to maximize the benefit of the cloud, providers must be free to move data through the cloud in the most efficient way.
- **Promoting security:** Users must be assured that cloud computing providers understand and properly manage the risks inherent in storing and running applications in the cloud. Cloud providers must be able to implement cutting-edge cybersecurity solutions without being required to use specific technologies.
- **Battling cybercrime:** In cyberspace, as in the real world, laws must provide meaningful deterrence and clear causes of action. Legal systems should provide an effective mechanism for law enforcement, and for cloud providers themselves, to combat unauthorized access to data stored in the cloud.
- **Protecting intellectual property:** In order to promote continued innovation and technological advancement, intellectual property laws should provide for clear protection and vigorous enforcement against misappropriation and infringement of the developments that underlie the cloud.
- **Ensuring data portability and the harmonization of international rules:** The smooth flow of data around the world — for example, between different cloud providers — requires efforts to promote openness and interoperability. Governments should work with industry to develop standards, while also working to minimize conflicting legal obligations on cloud providers.
- **Promoting free trade:** By their very nature, cloud technologies operate across national boundaries. The cloud's ability to promote economic growth depends on a global market that transcends barriers to free trade, including preferences for particular products or providers.
- **Establishing the necessary IT infrastructure:** Cloud computing requires robust, ubiquitous, and affordable broadband access. This can be achieved through policies that provide incentives for private sector investment in broadband infrastructure and laws that promote universal access to broadband.

The move to the cloud and capitalization on its benefits across the board is hardly inevitable, and an urgent task lies ahead for governments. In order to obtain the benefits of the cloud, policymakers must provide a legal and regulatory framework that will promote innovation, provide incentives to build the infrastructure to support it, and promote confidence that using the cloud will bring the anticipated benefits without sacrificing expectations of privacy, security, and safety.

---

***The United States continues to be an active participant in international standards development processes and an advocate of free trade and harmonization.***

---

**Some countries made significant gains but little overall improvement:**

- ➔ Although many of the lower-achieving countries made big gains in some policy areas, the effect was dampened by other low scores. The strong intellectual property and IT readiness scores of Indonesia, Thailand and Vietnam, for example, were negatively off-set by poor scores in security.
- ➔ Brazil typifies the struggle of these countries. Brazil ranked lowest in 2012. Although this year it improved considerably, its position in the rankings (22nd) remains the same as it was in the last Scorecard. Despite improvements in security, infrastructure and Internet freedom, Brazil is held back by a lack of comprehensive privacy laws, out-of-date copyright laws, gaps in intellectual property protection and widespread online piracy.

**In the world's largest markets, countries remained stable with modest gains:**

- ➔ Japan remains in first place, with a score made stronger by continual update and reform of privacy laws, among other policies.
- ➔ Canada made the biggest jump in rank, moving up five spots (for a total of eight positions since the first Scorecard in 2012) into fourth place. Canada's score benefits from a comprehensive privacy scheme with no onerous registration requirements.
- ➔ Of the six European Union countries considered in the Scorecard, all but the United Kingdom improved or held their positions since 2013. Specifically, Poland (4.70-point increase) and Italy (3.81) each moved up two positions in the rankings, while Germany (2.96)

and France (2.41) moved up one place and Spain (2.55) stayed the same. The United Kingdom's score increased by 1.94 points, but the country lost two places in the rankings due to the gains of other countries. The EU continues to develop regulations that will likely improve harmonization of laws across Europe and increase their scores — so long as the regulations do not also create new burdens.

- ➔ The United States achieved a 2.64-point increase, thanks to a significant improvement in free trade policies and improved IT infrastructure. The United States moved up one position into second place behind Japan. The United States continues to be an active participant in international standards development processes and an advocate of free trade and harmonization.
- ➔ Despite their cloud-readiness, there remains a strong need among the higher-ranked countries for the alignment of legal and regulatory environments that will allow for cloud computing's global potential and provide a model toward which other countries can strive.

**General improvements in global IT infrastructure continue, but the picture is uneven:**

- ➔ Most countries have improved their infrastructure score significantly since the last Scorecard, with the biggest improvers being France, Russia, South Africa, Thailand and the United Kingdom. Several countries, including Japan, Korea and Singapore, have implemented impressive national broadband networks.
- ➔ Despite major infrastructure improvements under way in a number of countries, broadband penetration remains very inconsistent.

# KEY FINDINGS

The 2016 BSA Global Cloud Computing Scorecard reveals significant changes in the policy environment for cloud computing in key global economies since the previous Scorecard in 2013. Many of the changes are positive, especially in the field of data protection and intellectual property protection.

General improvements in global IT infrastructure have produced a positive environment for cloud computing. However, some countries have lost ground due to new restrictions on IT service providers, and new trade barriers that threaten further growth and innovation in the cloud computing sector.

The findings are based on a unique examination and ranking of the 24 countries that account for 80 percent of the global IT market. Countries are scored across seven policy areas encompassing the laws, regulations and IT infrastructure necessary for the support and growth of digital technology and cloud computing.

## Data Privacy

Users of cloud computing continue to be concerned with the protection of private information they store in the cloud. The revelations regarding widespread national security surveillance have increased scrutiny of the issue and its scope.

Cloud users need to trust that their data, which may be stored anywhere in the world, will not be used or disclosed by a cloud provider in unauthorized ways. Countries can provide these assurances with appropriate privacy laws. But it is a delicate balance: unnecessarily burdensome restrictions will hinder the important advantages of cloud computing that users want and need.

This section of the Scorecard examines how countries are managing these competing interests. Overall, the concern for privacy has produced many positive results around the globe, including significant law reform, greater oversight of national security agencies, a strengthening of security and encryption regimes by key cloud service providers and a greater public awareness of data privacy issues.

But in some nations, governments have proposed stronger restrictions on the cross-border transfer of data without further benefits. If those proposals become law, they could negatively impact cloud service providers.

Since 2013, most countries have data protection frameworks in place and have established independent privacy commissioners. Many of the protection laws are based on the Organisation for Economic Co-operation and Development Guidelines, the European Union Data Protection Directive and the Asia-Pacific Economic Cooperation Privacy Principles.

However, some countries still have registration requirements for data controllers and cross-border data transfers in place, and a small number of countries have adopted or proposed prescriptive data localization regimes that would require cloud providers to restrict the free flow of data or build costly — and unnecessary — servers in order to provide services in a specific market.



## CASE STUDY

### **MODERNIZING TRADE RULES: Trans-Pacific Partnership Pact Eases Data Sharing**

The 21st century will be defined by explosive growth in digital trade. Every year, more businesses and their customers are using data services — including storage, processing and analytics — much of it through cloud computing.

Software and data services have transformed the lives of millions of people around the world. Farmers use analytics to reduce the use of pesticides and water and improve yields; cities use data to design transportation routes that save time and reduce emissions; and doctors employ data analysis to speed up diagnoses for their patients and increase the effectiveness of treatments.

But while digital trade has been rapidly evolving, trade rules have not kept up. Multilateral trade agreements currently in force do not contemplate the rapid technological advances that have occurred in recent years, including the scope and potential of cloud computing technology. It is an area of growing concern because the digital economy needs a positive policy environment to continue growing.

The good news is that in October of 2015 an important development occurred: 12 countries<sup>1</sup> announced the conclusion of the negotiation of the Trans-Pacific Partnership Agreement, known as TPP.<sup>2</sup>

The TPP is a milestone as it represents the first multilateral trade agreement to create a strong framework for the movement of data across borders. Among its key provisions, the signatories agree that they “shall allow” the cross-border transfer of information by electronic means, subject to a limited public policy exception, and they will not require the presence of local computing facilities as a prerequisite for access to their national markets. Also, they will not mandate source code disclosure for market access, and they will not impose customs duties on electronic transmissions.

The final provisions are expected to align and considerably improve digital trade policies among the participating nations. Since these countries account for 40 percent of the global economy, the potential positive impact of the TPP cannot be overestimated.

The TPP is an important step in the right direction. It also paves the way for other digital trade agreements, such as the Trade in Services Agreement (TiSA), which currently has 23 countries at the negotiating table. TiSA seeks to open markets and improve rules in areas such as licensing, financial services, telecoms, e-commerce and maritime transport.

Multilateral trade agreements may take time, effort and compromise to complete, but they deliver benefits that go far beyond the negotiating table. In the case of the TPP, the result is a bigger, healthier cloud for users of every size and need.

---

<sup>1</sup> When TPP negotiations were concluded, the participating countries were Australia, Canada, Japan, Malaysia, Mexico, Singapore, the United States and Vietnam (all of which are countries covered by this report), Brunei, Chile, New Zealand and Peru. Other countries may join TPP in the future.

<sup>2</sup> As of January 2016, TPP signature and implementation is still pending.

Canada and Korea have the highest score in the privacy section, offering comprehensive privacy regimes with no onerous registration requirements. Because Japan continues to update and reform its privacy laws, it also scores well in this section. South Africa received a big boost to its score and ranking for introducing a comprehensive privacy regime.

Unfortunately, privacy laws are still absent or insufficient in several countries. Brazil, Thailand and Turkey have no comprehensive laws in place, while laws in China, India, Indonesia and Vietnam remain very limited.

One notable development is the introduction of a new data protection framework in Russia containing prescriptive data localization requirements, such as a new law requiring that the personal data of Russian citizens be stored on servers based in Russia. This new regime is likely to act as a significant barrier to cloud service providers, and Russia's score and ranking fell as a direct result.

Privacy laws in the European Union and the United States continue to be the subject of significant debate and reform. The EU is close to the final implementation of a new regulation. The proposed General Data Protection Regulation (GDPR) contains many positive elements, and it should drive improved harmonization of laws across Europe. But the proposed regulation presents some challenges and potential administrative burdens for cloud service providers, including its liability regime, extension of data processor burdens, and the potential for jurisdictional clashes on access to data by authorities.

**(Editor's note:** Following the completion of the research underlying this year's research, the United States and European Union have continued to move closer to finalizing a new agreement, the Privacy Shield, that will allow data to continue to be shared across borders. This is an important development that was not finalized in time to fully be considered for this report.)

In the United States, officials have not made significant progress on development of general privacy legislation, but work has increased on improving oversight of national security agencies and improving legal redress avenues for overseas data subjects.

---

***Overall, many countries have responded to emerging threats to cybersecurity by developing and implementing new cybersecurity frameworks, laws and policies.***

---

## Security

Users of cloud computing and other digital services need to be certain that cloud service providers can manage the security risks of storing their data and running their applications on cloud systems. These concerns have been intensified by a number of recent high-profile, international cybersecurity attacks, including breaches that range across the economy, from health insurance providers to hotel chains and even toymakers.

This section examines how countries regulate security criteria and test security measures. It also examines the status of electronic signature laws and the Internet censorship or filtering requirements some countries are imposing with a view to stemming certain Internet-related crimes. Overall, many countries have responded to emerging threats to cybersecurity by developing and implementing new cybersecurity frameworks, laws and policies.

The Scorecard indicates that most countries now have security requirements in place. Most also now have clear, technology-neutral electronic signature laws. Overall, cybersecurity scores have risen significantly when compared with the last Scorecard.

France, Japan, Italy, the United Kingdom and the United States all score well in this section. China, Indonesia, Malaysia and Vietnam score poorly.

The Scorecard also reveals some overly prescriptive security requirements that duplicate accepted international standards and/or impose onerous local requirements. For example, Russia requires service providers to locate their data centers inside the country, and several countries have introduced local security testing requirements.





## CASE STUDY

### **RUSSIA: The Negative Impact of New Data Localization Policies**

Cloud computing and data analytics deliver enormous benefits to governments, consumers and businesses, enhancing lives and spurring unprecedented economic growth.

Unfortunately, some countries are now adopting, or contemplating, data localization policies that threaten to destroy the gains and growth potential of software and data-driven innovations such as cloud computing.

Computer networks store and process data in multiple locations in multiple countries. But data localization policies require service providers — and the data they manage — to be located inside the country where their services are accessed. These “walled-off” providers can no longer contribute to or receive the benefits of the global cloud.

Russia is one such country that recently adopted a data localization law. In September 2015, Russia mandated that all companies serving the Russian market must process and store Russian citizens’ personal data in databases located inside the country. In enacting the law, the government cited the need to protect Russian citizens from unlawful access to their data by foreign governments.

But data localization laws are not an effective mechanism for protecting citizen information. Data are not kept safer by virtue of being kept in a specific location. The ideal method for keeping data secure is the use of robust security technology, processes and controls, and data protection legislation coupled with effective enforcement. If there are concerns regarding mandatory disclosures required by foreign governments, these are best served through international cooperation versus isolation.

Not only are data localization laws ineffective, they deter essential economic growth and innovation. Many companies will be unable or unwilling to operate in countries with data localization requirements due to the complexity and extremely high associated costs. Most companies — even the very large ones — are simply not able to build and maintain servers in every country they serve.

Although it is too early to evaluate the full ramifications of the new Russian law, there is little doubt that it will impact Russian consumers and the Russian economy. The European Center for International Political Economy has estimated that the law will cost the country around 0.27 percent of its GDP.<sup>3</sup>

Data localization requirements cannot be ignored. They compromise access to globalized supply chains and negatively impact investments, exports and economic growth — not just for the country that imposes them, but for the global digital economy as a whole.

---

<sup>3</sup> The report “Data Localisation in Russia: A Self-imposed Sanction” may be found at <http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/>.

Several countries also continue to impose Internet filtering or censorship regimes that may act as barriers to the expansion of the digital economy and cloud computing. The intention of the schemes may be to address criminal conduct, including distribution of illegal material such as child pornography, but some are blocking sites that express political dissent.

## Cybercrime

Because the massive quantities of valuable data held in cloud-computing data centers have attracted the attention of organized crime, governments must address these ever-evolving threats with robust legislation, investigation and enforcement.

This section examines cybercrime laws, as well as rules relating to investigation and enforcement, which includes access to encrypted data by investigators and the prosecution of extraterritorial offenses.

Overall, the Scorecard indicates that most countries are rising to the challenge of protecting data from cyberattack and physical security breaches. Most have legislation combatting the unauthorized access of data stored in the cloud. Most also have now implemented computer crime laws or cybercrime laws, many of which are broadly compliant with the Convention on Cybercrime.

Indeed, many countries in the study — Australia, Canada, EU Member States, Japan and the United States — have now ratified the convention. Australia, France, Germany and Japan score extremely high results in the cybercrime section.

Unfortunately, a few key jurisdictions still have gaps and inconsistencies in their cybercrime laws. China, Korea, Russia and Vietnam scored poorly.

Countries diverge when it comes to enforcement, investigation and prosecution of cybercrime. In particular, many countries are debating the extent to which law enforcement should be allowed access to encrypted data. The resolution of these issues and their impact on global policy remains to be seen.

---

**Overall, the Scorecard indicates that most countries are rising to the challenge of protecting data from cyberattack and physical security breaches.**

---

## Intellectual Property Rights

As with other highly innovative and fast-evolving products, providers of cloud computing services rely on a combination of patents, copyrights, trade secrets and other forms of intellectual property protection. To encourage investment in cloud research and development, intellectual property laws must provide clear protections and vigorous enforcement of misappropriation and infringement. Online intermediaries should be offered incentives to operate responsibly and should enjoy safe harbor from copyright liability when they do so.

This section examines the intellectual property protections in place in each country, as well as their investigatory and enforcement approaches.

Overall, the Scorecard reveals significant reform in intellectual property laws since the last Scorecard, although gaps and inconsistencies still exist, especially with regard to enforcement.

Australia, Italy and Korea received the highest scores for intellectual property protection due to their robust legislative schemes. Canada updated and improved its intellectual property laws. Significant gaps in the laws of Brazil and Vietnam left these countries with the poorest results.

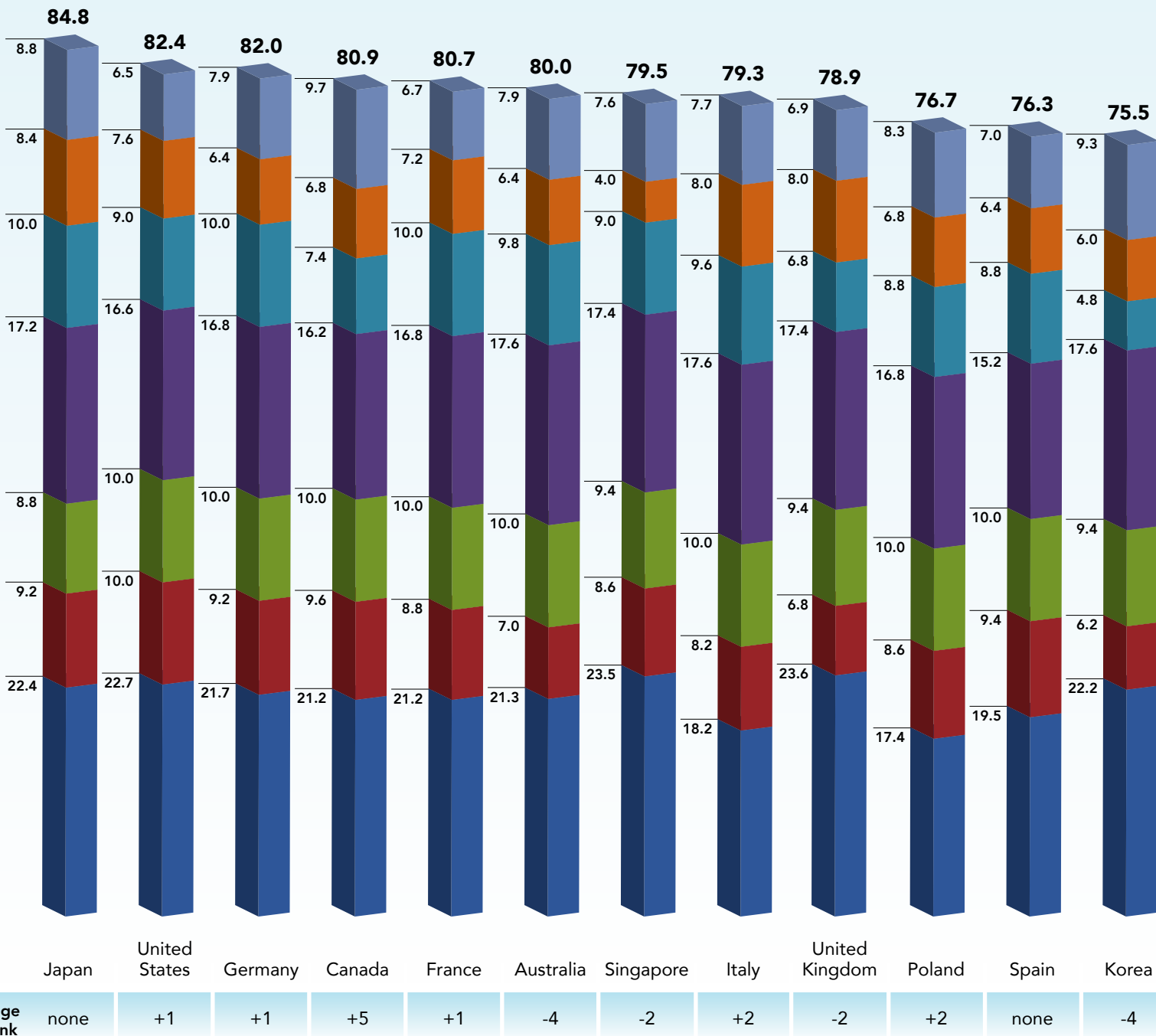
## Support for Industry-Led Standards and International Harmonization of Rules

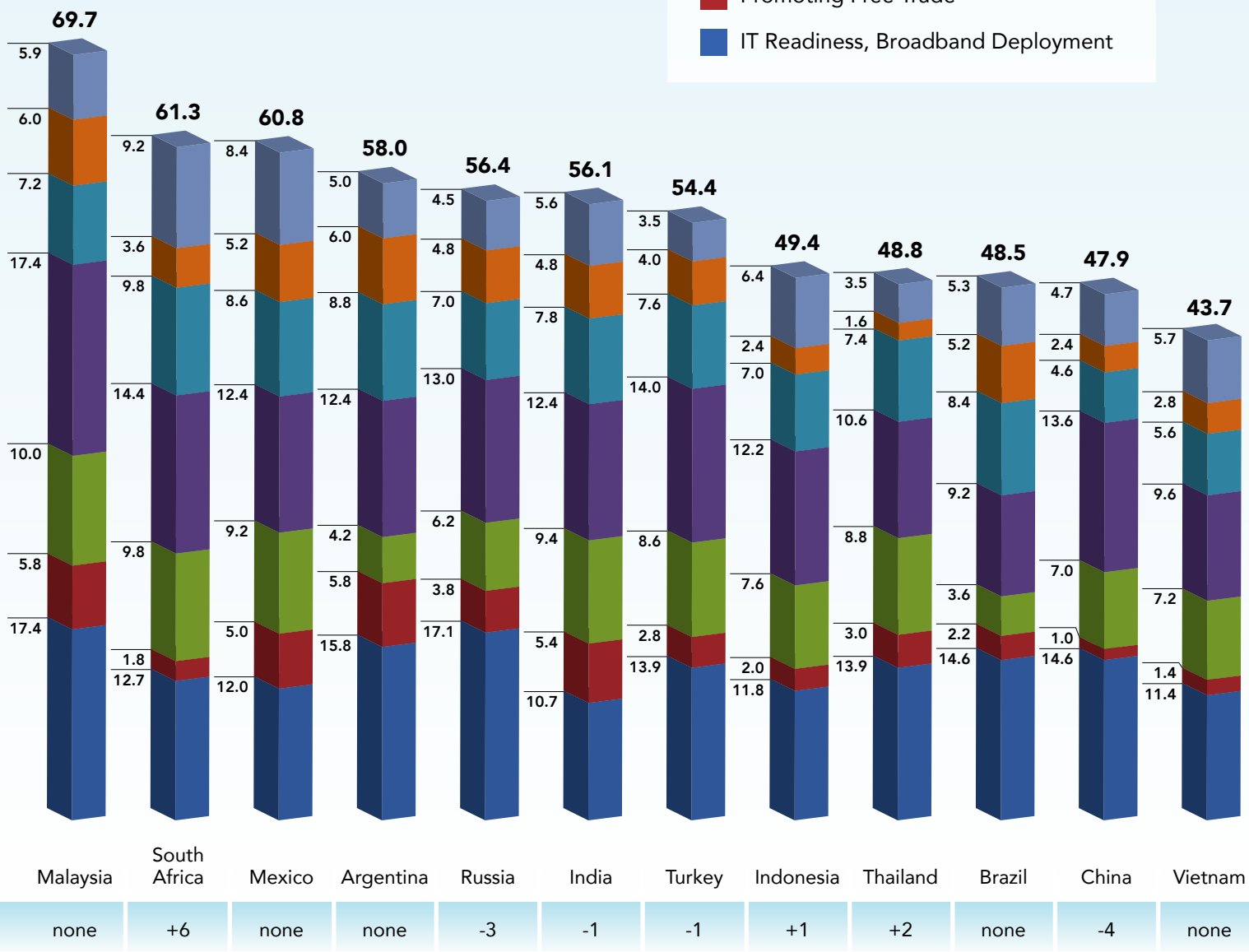
Users need data portability and seamless interoperable applications if they are to make full use of cloud-computing services and the digital economy. IT industry organizations are developing international standards that will ensure optimal portability. Government support for these voluntary, industry-led efforts is

*continued on page 12*

# 2016 BSA Global Cloud Computing Scorecard

Several countries have made marked improvements in the policy environment for cloud computing in the past year. These findings are based on the BSA Scorecard's one-of-a-kind examination and ranking of 24 countries that account for 80 percent of the global IT market.





---

***Despite major infrastructure improvements under way in a number of countries, broadband penetration remains very inconsistent.***

---

highly important. Countries must also promote global harmonization of e-commerce rules, tariffs and relevant trade rules.

This section examines the extent to which governments have encouraged industry-led processes and promoted harmonization of e-commerce rules.

The Scorecard reveals that some countries have moved away from accepting international standards and international certifications, most notably China, India, Indonesia, Korea and Russia.

Although tariffs and trade barriers for online software and applications continue to be rare, they are still hindering new technology products used to access cloud services in a few countries. Argentina, Brazil and Russia all scored poorly in this section.

### **Promoting Free Trade**

Cloud services operate across national boundaries, and their success depends on access to regional and global markets. Restrictive policies that create actual or potential trade barriers will inhibit or slow the evolution of cloud computing.

This section examines government procurement regimes and the existence or absence of barriers to free trade, including each country's requirements and preferences for particular products. The section also examines whether countries have joined the World Trade Organization Agreement on Government Procurement, which liberalizes such policies.

The Scorecard reveals that a number of countries still provide preferential treatment for domestic suppliers in government procurement, or have introduced other barriers to international trade. Vietnam and China recorded the lowest scores, while Canada and the United States scored the highest.

### **IT Readiness and Broadband Deployment**

Digital economies and cloud computing require extensive, affordable broadband access, which in turn requires incentives for private sector investment in infrastructure and laws and policies that support universal access.





This section of the Scorecard examines and compares the infrastructure available in each country to support the digital economy and cloud computing. It is based on detailed comparative statistics on a range of important IT indicators, including the presence of a national broadband plan, a country's International Connectivity Score and International Internet Bandwidth. In addition, the Scorecard includes statistics on the number of subscribers for various services, reflecting the importance (and growth) of mobile broadband subscriptions.

Overall, most countries have improved their infrastructure score significantly since the last Scorecard, with the biggest improvers being France, Russia, South Africa, Thailand and the top-scoring United Kingdom. Several countries, including Japan, Korea and Singapore, have high scores reflecting their implementation of impressive national broadband networks.

Despite major infrastructure improvements under way in a number of countries, broadband penetration remains very inconsistent. As a result, some countries continue to have low infrastructure scores. Countries that do not yet have sufficient infrastructure continue to be at risk of missing the economic benefits of the digital economy and cloud computing.

# SCORECARD METHODOLOGY

The BSA Global Cloud Computing Scorecard examines the legal and regulatory framework of 24 countries around the world, identifying 66 questions that are relevant to determining readiness for cloud computing. The questions are categorized under the aforementioned policy categories, and are generally framed so as to be answerable by “yes” or “no.” The answers are also color coded:

-  Indicates a positive assessment, which is generally considered to be an encouraging step toward the establishment of a favorable legal and regulatory environment for cloud computing.
-  Indicates a negative assessment and the presence of a potential barrier to the establishment of a favorable legal and regulatory environment for cloud computing.
-  Indicates that the assessment is positive in part, although some gaps or inconsistencies may exist that require further remedial work.
-  Indicates a fact-finding question on relevant issues.

The Scorecard aims to provide a platform for discussion between policymakers and providers of cloud offerings, with a view toward developing an internationally harmonized regime of laws and regulations relevant to cloud computing. It is a tool that can help policymakers conduct a constructive self-evaluation, and determine the next steps that need to be taken to help advance the growth of global cloud computing.

Responses for the infrastructure portion of the Scorecard are color coded based on the scale below. That is, the “highest” answer to a particular question (e.g., the largest population or highest number of Internet users) is indicated in bright green, and the color for other responses graduates down to the lowest response in red.

## IT Readiness (Country Ranking Out of 24)



# USING THE SCORECARD

The Scorecard is derived from the Country Reports — a weighted score has been allocated to a selection of key questions. A number of basic fact-finding questions are excluded from the scoring system. Each group of questions is weighted to reflect its importance to cloud computing. Each individual question is also weighted to reflect its importance within each group. The weights are shown in the following table:

# THEME / QUESTIONS	Weight	Value (out of 100)
<b>DATA PRIVACY</b>	<b>10%</b>	<b>10</b>
1. Are there laws or regulations governing the collection, use or other processing of personal information?	30%	3
6. Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	25%	2.5
8. Are data controllers free from registration requirements?	20%	2
9. Are cross-border transfers free from registration requirements?	15%	1.5
10. Is there a breach notification law?	10%	1
<b>SECURITY</b>	<b>10%</b>	<b>10</b>
1. Is there a law or regulation that gives electronic signatures clear legal weight?	20%	2
2. Are ISPs and content service providers free from mandatory filtering or censoring?	20%	2
3. Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	20%	2
4. Are there laws or enforceable codes containing specific security audit requirements for digital data hosting and cloud service providers?	20%	2
5. Are there security laws and regulations requiring specific certifications for technology products?	20%	2
<b>CYBERCRIME</b>	<b>10%</b>	<b>10</b>
1. Are there cybercrime laws in place?	50%	5
2. Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	30%	3
3. What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers or other service providers?	10%	1
4. How does the law deal with extraterritorial offenses?	10%	1
<b>INTELLECTUAL PROPERTY RIGHTS</b>	<b>20%</b>	<b>20</b>
1. Is the country a member of the TRIPS Agreement?	10%	2
2. Have IP laws been enacted to implement TRIPS?	10%	2
3. Is the country party to the WIPO Copyright Treaty?	10%	2
4. Have laws implementing the WIPO Copyright Treaty been enacted?	10%	2
5. Are civil sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	10%	2
6. Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	10%	2
7. Are there laws governing ISP liability for content that infringes copyright?	5%	1
8. Is there a basis for ISPs to be held liable for content that infringes copyright found on their sites or systems?	5%	1
10. Must ISPs take down content that infringes copyright, upon notification by the copyright holder?	5%	1
11. Are ISPs required to inform subscribers upon receiving a notification that the subscriber is using the ISP's service to distribute content that infringes copyright?	5%	1
12. Is there clear legal protection against misappropriation of cloud computing services, including effective enforcement?	20%	4

# THEME / QUESTIONS	Weight	Value (out of 100)
<b>SUPPORT FOR INDUSTRY-LED STANDARDS &amp; INTERNATIONAL HARMONIZATION OF RULES</b>	<b>10%</b>	<b>10</b>
1. Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	30%	3
2. Is there a regulatory body responsible for standards development for the country?	10%	1
3. Are e-commerce laws in place?	30%	3
5. Is the downloading of applications or digital data from foreign cloud service providers free from tariff or other trade barriers?	10%	1
6. Are international standards favored over domestic standards?	10%	1
7. Does the government participate in international standards-setting process?	10%	1
<b>PROMOTING FREE TRADE</b>	<b>10%</b>	<b>10</b>
1. Are there any laws or policies in place that implement technology neutrality in government?	20%	2
2. Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	20%	2
3. Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?	10%	1
4. Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	50%	5
<b>IT READINESS, BROADBAND DEPLOYMENT</b>	<b>30%</b>	<b>30</b>
1. Is there a national broadband plan?	13%	3.75
3.7 Personal Computers (% of households) (2014)	3%	0.75
4.1 ITU ICT Development Index (IDI) (2015) (Score is out of 10 and includes 167 countries)	20%	6
4.2 World Economic Forum Networked Readiness Index (NRI) (2015) (Score is out of 7 and includes 143 countries)	20%	6
4.3 International Connectivity Score (2014) (Score is out of 10 and includes 50 countries)	15%	4.5
4.4 IT Industry Competitiveness Index (2011) (Score is out of 100 and includes 66 countries) (Note: This is not as current as the other indicators and while it is no longer displayed in the reports it has been retained as part of the overall score for integrity and consistency purposes)	10%	3
5.2 Internet Users as Percentage of Population (2014)	5%	1.5
5.3 International Internet Bandwidth (2014) (bits per second per Internet user)	3%	0.75
5.4 International Internet Bandwidth (2014) (total gigabits per second [Gbps] per country)	3%	0.75
6.4 Fixed Broadband Subscriptions as % of Internet Users (2014)	5%	1.5
7.2 Active Mobile Broadband Subscriptions per 100 Inhabitants (2014)	5%	1.5



# BSA Global Cloud Computing Country Checklist

✓ Yes ✗ No ⦿ Partial

# QUESTION	Argentina	Australia	Brazil
<b>DATA PRIVACY</b>			
1. Are there laws or regulations governing the collection, use, or other processing of personal information?	✓	✓	⦿
2. What is the scope and coverage of privacy law?	Comprehensive	Comprehensive	Not applicable
3. Is the privacy law compatible with the Privacy Principles in the EU Data Protection Directive?	✓	⦿	✗
4. Is the privacy law compatible with the Privacy Principles in the APEC Privacy Framework?	✓	✓	✗
5. Is an independent private right of action available for breaches of data privacy?	Available	Not available	Available
6. Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	National regulator	National regulator	None
7. What is the nature of the privacy regulator?	Sole commissioner	Sole commissioner	Not applicable
8. Are data controllers free from registration requirements?	✗	✓	✓
9. Are cross-border transfers free from registration requirements?	⦿	✓	✓
10. Is there a breach notification law?	✗	✗	✗
<b>SECURITY</b>			
1. Is there a law or regulation that gives electronic signatures clear legal weight?	✓	✓	✓
2. Are ISPs and content service providers free from mandatory filtering or censoring?	✓	✓	✓
3. Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	Limited coverage in legislation	Limited coverage in legislation	Limited coverage in legislation
4. Are there laws or enforceable codes containing specific security audit requirements for digital data hosting and cloud service providers?	Limited coverage in legislation	None	Limited coverage in legislation
5. Are there security laws and regulations requiring specific certifications for technology products?	No requirements	Limited requirements	No requirements
<b>CYBERCRIME</b>			
1. Are cybercrime laws in place?	✓	✓	✓
2. Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	✓	✓	✓
3. What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers or other service providers?	Access with a warrant	Access with a warrant	Access with a warrant
4. How does the law deal with extraterritorial offenses?	Limited coverage	Comprehensive coverage	Comprehensive coverage
<b>INTELLECTUAL PROPERTY RIGHTS</b>			
1. Is the country a member of the TRIPS Agreement?	✓	✓	✓
2. Have IP laws been enacted to implement TRIPS?	✓	✓	✓
3. Is the country party to the WIPO Copyright Treaty?	✓	✓	✗
4. Have laws implementing the WIPO Copyright Treaty been enacted?	⦿	✓	⦿
5. Are civil sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	⦿	✓	⦿
6. Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	⦿	✓	⦿
7. Are there laws governing ISP liability for content that infringes copyright?	✗	⦿	⦿
8. Is there a basis for ISPs to be held liable for content that infringes copyright found on their sites or systems?	✗	✓	⦿
9. What sanctions are available for ISP liability for copyright infringing content found on their site or system?	Not applicable	Civil and criminal	Civil
10. Must ISPs take down content that infringes copyright, upon notification by the right holder?	⦿	✓	✗
11. Are ISPs required to inform subscribers upon receiving a notification that the subscriber is using the ISP's service to distribute content that infringes copyright?	✗	✓	✗
12. Is there clear legal protection against misappropriation of cloud computing services, including effective enforcement?	Limited protection (criminal activity only)	Comprehensive protection	Limited protection (criminal activity only)
<b>SUPPORT FOR INDUSTRY-LED STANDARDS &amp; INTERNATIONAL HARMONIZATION OF RULES</b>			
1. Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	✗	✓	✗
2. Is there a regulatory body responsible for standards development for the country?	✓	✓	✓
3. Are e-commerce laws in place?	⦿	✓	✗
4. What international instruments are the e-commerce laws based on?	Not applicable	UNCITRAL Model Law on E-Commerce	Not applicable
5. Is the downloading of applications or digital data from foreign cloud service providers free from tariff or other trade barriers?	✗	✓	✗
6. Are international standards favored over domestic standards?	⦿	✓	✓
7. Does the government participate in international standards setting process?	✓	✓	✓





North Africa	Spain	Thailand	Turkey	United Kingdom	United States	Vietnam
✓	✓	✗	✗	✓	🕒	🕒
Comprehensive	Comprehensive	Not Applicable	Not Applicable	Comprehensive	Sectoral	Sectoral
✓	✓	✗	✗	✓	🕒	🕒
✓	✓	✗	✗	✓	🕒	🕒
Available	Available	Available	Available	Available	Available	Available
National regulator	National regulator	None	None	National regulator	Sectoral regulator	None
Commissioner	Sole commissioner	Not applicable	Not applicable	Sole commissioner	Other government official	Not applicable
✓	✗	✓	✓	✗	✓	✓
✓	✗	✓	✓	✓	🕒	✓
✓	🕒	✗	✗	🕒	✓	🕒
✓	✓	✓	✓	✓	✓	✓
✓	✓	✗	✗	✓	✓	✗
Limited coverage in legislation	Limited coverage in legislation	None	None	Limited coverage in legislation	Limited coverage in legislation	Limited coverage in legislation
None	None	None	None	Limited coverage in legislation	Limited coverage in legislation	None
Requirements	Comprehensive requirements (including Common Criteria)	No requirements	Comprehensive requirements (including Common Criteria)	Comprehensive requirements (including Common Criteria)	Comprehensive requirements (including Common Criteria)	No requirements
✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	🕒	✓	🕒
Access with a warrant	Not stated	Unlimited access	Unlimited access	Unlimited access	Access with a warrant	Unlimited access
Comprehensive coverage	Comprehensive coverage	Comprehensive coverage	Limited coverage	Comprehensive coverage	Limited coverage	Limited coverage
✓	✓	✓	✓	✓	✓	✓
✓	✓	🕒	✓	✓	✓	🕒
✗	✓	✗	✓	✓	✓	✗
🕒	✓	🕒	✓	✓	✓	🕒
✓	🕒	✓	✓	✓	🕒	✓
✓	✓	✓	✓	✓	✓	🕒
✓	✓	✓	✓	✓	✓	🕒
Civil	Civil	Civil and criminal	Civil and criminal	Civil and criminal	Civil and criminal	Not applicable
✓	✓	🕒	✓	🕒	✓	✗
✗	✗	✗	✗	🕒	🕒	✗
Comprehensive protection	Comprehensive protection	Comprehensive protection	Comprehensive protection	Comprehensive protection	Comprehensive protection	Comprehensive protection
✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	🕒	✓	✓	✓
UNCITRAL Model Law on E-Commerce	UNCITRAL Model Law on E-Commerce	UNCITRAL Model Law on E-Commerce	Other	UNCITRAL Model Law on E-Commerce	Other	UNCITRAL Model Law on E-Commerce
✓	✓	✓	✓	✓	✓	✗
✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓	✓

# QUESTION	Argentina	Australia	Brazil
<b>PROMOTING FREE TRADE</b>			
1. Are there any laws or policies in place that implement technology neutrality in government?	✘	✔	✘
2. Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	✔	✔	✔
3. Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?	✔	✔	🕒
4. Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	🕒	🕒	✘
<b>IT READINESS, BROADBAND DEPLOYMENT</b>			
1. Is there a national broadband plan?	<ul style="list-style-type: none"> <li>By 2015, more than 10 million homes with broadband access</li> <li>By 2015, 97% of the population accessing an optical fiber network at 10 Mbps and the remaining 3% of the population covered by satellite connections</li> </ul>	<ul style="list-style-type: none"> <li>By 2020, the National Broadband Network (NBN) is forecasted to provide 8 million connections at speeds of 25–50 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>By 2019, national average broadband speed being Mbps</li> </ul>
2. Are there laws or policies that regulate the establishment of different service levels for data transmission based on the nature of data transmitted?	Multiple regulations and limited public debate	No regulation and extensive public debate	Multiple regulations and extensive public debate
<b>3. Base Indicators</b>			
3.1. Population (millions) (2014)	41	23	200
3.2. Urban Population (%) (2014)	92%	89%	85%
3.3. Number of Households (millions) (2014)	11	9	59
3.4. Population Density (people per square km) (2014)	16	3	25
3.5. Per Capita GDP (US\$ 2014)	\$12,569	\$61,887	\$11,388
3.6. IT Service Exports (2014) (billions of US\$)	\$5.8	\$9.9	\$23.0
3.7. Personal Computers (2014) (% of households)	62%	86%	52%
<b>4. IT and Network Readiness Indicators</b>			
4.1. ITU ICT Development Index (IDI) (2015) (Score is out of 10 and covers 167 countries)	6.40	8.29	6.03
4.2. World Economic Forum Networked Readiness Index (NRI) (2015) (Score is out of 7 and covers 143 countries)	3.72	5.48	3.85
4.3. International Connectivity Score (2014) (Score is out of 10 and covers 52 countries)	4.50	5.37	4.83
<b>5. Internet Users and International Bandwidth</b>			
5.1. Internet Users (millions) (2014)	25	19	103
5.2. Internet Users as Percentage of Population (2014)	60%	83%	52%
5.3. International Internet Bandwidth (2014) (bits per second per Internet user)	48,065	75,069	42,966
5.4. International Internet Bandwidth (2014) (total gigabits per second [Gbps] per country)	1,300	1,500	5,000
<b>6. Fixed Broadband</b>			
6.1. Fixed Broadband Subscriptions (millions) (2014)	6	6	20
6.2. Fixed Broadband Subscriptions as % of households (2014)	52%	65%	34%
6.3. Fixed Broadband Subscriptions as % of population (2014)	16%	28%	12%
6.4. Fixed Broadband Subscriptions as % of Internet users (2014)	24%	30%	20%
<b>7. Mobile Broadband</b>			
7.1. Mobile Cellular Subscriptions (millions) (2014)	66	31	281
7.2. Active Mobile Broadband Subscriptions per 100 inhabitants (2014)	54	112	78
7.3. Number of Active Mobile Broadband Subscriptions (millions) (2014)	22	27	158

IT Readiness (Country Ranking Out of 24)



	Canada	China	France	Germany	India	Indonesia	Italy
	✓	✗	🕒	✓	🕒	🕒	🕒
	✓	✗	✓	✓	🕒	🕒	✓
	✓	✗	🕒	🕒	✗	🕒	✗
	✓	🕒	✓	✓	🕒	✗	✓
ational adband g 25	<ul style="list-style-type: none"> <li>By 2017, all Canadians to have access to broadband speeds of at least 5 Mbps for downloads and 1 Mbps for uploads</li> </ul>	<ul style="list-style-type: none"> <li>By 2020: <ul style="list-style-type: none"> <li>Coverage will reach 70% of households</li> <li>Fiber to the home connections will surpass 300 million</li> <li>Urban Internet speeds: 50 Mbps</li> <li>Rural Internet speeds: 12 Mbps</li> <li>Expected 400 million fixed broadband subscriptions</li> <li>3G and 4G wireless coverage to 85% of households</li> <li>Expected 1.3 billion 3G/4G customers</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>By 2022, 100% coverage of broadband connections providing in excess of 30 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>By 2018, households to have speeds of at least 50 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>By 2016, fiber network to reach 250,000 local government areas</li> </ul>	<ul style="list-style-type: none"> <li>By 2019: <ul style="list-style-type: none"> <li>71% of urban and 10% of rural households connected to fixed broadband, at speeds of 20 Mbps</li> <li>100% of business buildings in urban areas connected to fixed broadband at speeds of 1 Gbps</li> <li>30% penetration rate of fixed broadband in urban areas; 6% in rural areas</li> <li>100% penetration of mobile broadband in urban areas and 52% in rural areas, at speeds of 1 Mbps</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>By 2020, deploy services with speeds of 100 Mbps to densely populated areas</li> <li>By 2020, deploy services with speeds of 30 Mbps to densely populated areas</li> </ul>
ulations e public e	Multiple regulations and extensive public debate	No regulation and limited public debate	Multiple regulations and extensive public debate	Regulation under consideration by government and extensive public debate	No regulation and extensive public debate	No regulation and limited public debate	Multiple regulations and extensive public debate
	35	1,386	64	83	1,252	250	61
	82%	54%	79%	75%	32%	53%	69%
	14	391	27	39	256	63	24
	4	145	121	232	436	140	209
5	\$50,271	\$7,594	\$42,733	\$47,627	\$1,596	\$3,492	\$34,960
	\$36.6	\$81.9	\$101.8	\$108.1	\$103.0	\$7.2	\$37.8
	88%	47%	83%	91%	13%	18%	74%
	7.76	5.05	8.12	8.22	2.69	3.94	7.12
	5.53	4.16	5.20	5.51	3.73	3.91	4.32
	5.27	3.40	5.04	5.42	2.14	2.89	3.76
	30	635	53	69	189	40	36
	86%	46%	82%	84%	15%	16%	58%
6	129,244	4,995	221,660	145,990	5,677	6,225	92,497
	4,000	3,433	12,000	10,400	1,295	270	3,500
	12	189	25	29	15	3	14
	86%	48%	94%	73%	6%	5%	58%
	35%	14%	40%	36%	1%	1%	24%
	39%	30%	47%	41%	8%	8%	38%
	29	1,286	65	100	944	326	94
	54	42	66	64	6	35	71
	19	583	43	53	70	88	43

	Japan	Korea	Malaysia	Mexico	Poland	Russia	Singapore
	🟡	🔴	🟡	🟢	🟢	🟡	🟢
	🟢	🟡	🟢	🟢	🟢	🔴	🟢
	🟢	🟢	🟡	🟢	🟢	🔴	🟢
	🟢	🟢	🟡	🔴	🟢	🟡	🟢
Needs addressed by government	<ul style="list-style-type: none"> <li>By 2015, all households to have very high-speed fiber broadband (FtTH) connections</li> </ul>	<ul style="list-style-type: none"> <li>By 2020, a fully operational commercial 5G broadband network</li> </ul>	<ul style="list-style-type: none"> <li>By 2020, 100% of households in capital cities and high-impact growth area to have access to speeds of 100 Mbps</li> <li>By 2020, 50% of households in suburban and rural areas to have access to speeds of 20 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>By 2018, a new national wireless broadband carrier network</li> </ul>	<ul style="list-style-type: none"> <li>By 2020, 100% of population to have access to speeds of at least 30 Mbps</li> <li>By 2025, 50% of households at 100 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>All settlements of over 250 people connected to a broadband network</li> <li>By 2015, 35% of the population to have broadband access</li> <li>By 2015, 75% of households to be connected to the Internet</li> </ul>	<ul style="list-style-type: none"> <li>By 2015, the Next-Generation National Broadband Network (Next-Gen NBN) to deliver 1 Gbps downstream and 500 Mbps upstream broadband access to every home, office and school</li> </ul>
Public debate	Limited regulation and extensive public debate	Limited regulation and extensive public debate	No regulation and extensive public debate	Multiple regulations and extensive public debate	Limited regulation and limited public debate	No regulation and limited public debate	Limited regulation and limited public debate
	127	49	30	122	38	143	5
	93%	82%	74%	79%	61%	74%	100%
	47	19	6	27	14	52	1
	349	517	91	65	124	9	7,736
	\$36,194	\$27,970	\$10,933	\$10,230	\$14,423	\$12,736	\$56,287
	\$40.6	\$23.5	\$13.3	—	\$13.8	\$21.2	\$38.1
	83%	78%	66%	38%	78%	71%	88%
	8.47	8.93	5.90	4.68	6.91	6.91	8.08
	5.60	5.52	4.85	4.03	4.38	4.53	6.02
	5.18	5.00	5.89	4.10	3.28	6.04	5.47
	110	42	20	53	24	88	4
	86%	85%	67%	43%	63%	61%	73%
	48,637	45,178	27,173	20,926	90,356	29,860	616,531
	5,595	1,886	554	1,150	2,300	3,000	2,789
	37	19	2	13	6	24	1
	78%	97%	39%	48%	44%	46%	114%
	29%	39%	10%	10%	19%	18%	27%
	34%	45%	12%	25%	25%	27%	36%
	153	57	45	102	57	221	8
	121	109	58	41	56	66	142
	154	54	18	51	21	94	8

South Africa	Spain	Thailand	Turkey	United Kingdom	United States	Vietnam
✗	✓	✗	✗	🕒	✓	✗
🕒	✓	✓	✓	✗	✓	✗
🕒	✓	✓	✓	✗	✓	✗
✗	✓	✗	✗	✓	✓	✗
<ul style="list-style-type: none"> <li>By 2016, 50% of population with access to speeds of 5 Mbps</li> <li>By 2020, 90% of population with access to speeds of 5 Mbps; 50% to speeds of 100 Mbps</li> <li>By 2030, 100% of population with access to speeds of 10 Mbps; 80% to speeds of 100 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>By 2020, 100% of population to have access to speeds of at least 30 Mbps</li> <li>By 2025, 50% of households at 100 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>By 2020, extend broadband coverage to 95%</li> <li>By 2020, provide broadband Internet access of at least 100 Mbps in economically important provinces</li> </ul>	<ul style="list-style-type: none"> <li>By 2018, the proportion of Internet users increase to 70%</li> <li>By 2018, the number of fiber Internet subscribers increase to 4 million</li> <li>By 2018, the number of LTE subscribers increase to 10 million</li> <li>By 2018, the proportion market share of alternative DSL operators increase to 25%</li> <li>By 2018, the GDP per capita rate of broadband access costs by lowered to 1%</li> </ul>	<ul style="list-style-type: none"> <li>By 2017, to bring "superfast broadband" to all parts of the UK with download speeds of at least 2 Mbps and to provide 95% of home and businesses with speeds of 24 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>By 2020, at least 100 million homes to have affordable access to download speeds of 100 Mbps and upload speeds of 50 Mbps</li> <li>By 2020, every household to have access to download speeds of 4 Mbps and upload speeds of 1 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>By 2015, 20–30% of households to have access to broadband</li> <li>By 2020, 50–60% of households have access to broadband, of which 20–30% access via fiber optic cable</li> </ul>
No regulation and limited public debate	Regulation under consideration by government and extensive public debate	No regulation and limited public debate	No regulation and limited public debate	Regulation under consideration by government and extensive public debate	Multiple regulations and extensive public debate	No regulation and limited public debate
53	47	67	75	63	320	92
64%	79%	49%	73%	82%	81%	33%
13	16	19	17	27	122	18
45	93	133	99	267	35	293
\$6,478	\$30,262	\$5,519	\$10,530	\$45,603	\$54,629	\$2,052
\$2.6	\$49.9	\$9.6	\$0.6	\$120.5	\$165.4	—
28%	74%	34%	56%	91%	81%	21%
4.90	7.66	5.36	5.58	8.75	8.19	4.28
3.99	4.73	4.05	4.41	5.62	5.64	3.85
3.94	4.33	3.69	4.13	5.90	6.46	3.57
26	34	19	35	57	269	40
49%	72%	29%	46%	90%	84%	44%
149,542	111,545	46,826	42,911	429,830	70,970	20,749
3,894	4,000	1,098	1,661	25,000	20,000	928
2	12	5	8	23	94	5
13%	75%	25%	49%	85%	77%	28%
3%	27%	8%	12%	37%	31%	6%
6%	36%	25%	24%	40%	35%	13%
79	51	97	72	78	356	136
47	77	80	43	89	103	31.04
25	36	54	32	56	331	29





## ABOUT BSA

BSA | The Software Alliance ([www.bsa.org](http://www.bsa.org)) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.

With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

## ABOUT GALEXIA

Galexia ([www.galexia.com](http://www.galexia.com)) is at the forefront of international research and advice in the areas of privacy, identity, cybersecurity and cloud — with a particular focus on global and cross-border legal and regulatory issues. The firm advises national governments, regional and global organizations (ASEAN and the United Nations), and the private sector (particularly ICT, health and financial services). The firm has expertise in the policy complexities that arise for countries and business addressing cross-border issues. Galexia publishes world-leading research publications, including the regular Cloud Scorecards, Cybersecurity Dashboards and reports on identity management, authentication, privacy and cyberlaws. The firm has specialist expertise in data governance, particularly the development and implementation of identity and authentication management systems, Privacy Impact Assessments and Cybersecurity strategies.

Galexia works closely with a range of international business and government clients to produce clear and effective outcomes from evidence based research. The firm uses collaborative cloud-based reporting tools to provide real-time access to our research and analysis.





[www.bsa.org](http://www.bsa.org)

**BSA Worldwide Headquarters**

20 F Street, NW  
Suite 800  
Washington, DC 20001

T: +1.202.872.5500  
F: +1.202.872.5501

**BSA Asia-Pacific**

300 Beach Road  
#25-08 The Concourse  
Singapore 199555

T: +65.6292.2072  
F: +65.6292.6369

**BSA Europe, Middle East & Africa**

2 Queen Anne's Gate Buildings  
Dartmouth Street  
London, SW1H 9BP  
United Kingdom

T: +44.207.340.6080  
F: +44.207.340.6090

# COUNTRY: INDIA

**SCORE: 56.08 | RANK: 18/24**

The law in India has not entirely kept pace with developments in cloud computing, and some gaps exist in key areas of protection; notably, India has not yet implemented effective privacy legislation.

India's cybercrime legislation also requires updating to conform to international models. Some laws and standards in India are not technology neutral (e.g., electronic signatures), and these may be a barrier to interoperability.




This year's report notes that India imposes some local security testing requirements in addition to international testing requirements. These local testing arrangements

have been the subject of criticism by India's trading partners, including the European Union.

However, copyright laws have improved in recent years, although India still has not ratified the WIPO Copyright Treaty.

The development of India's technology sectors remains challenging, with low levels of broadband and personal computer penetration.

Overall, India's ranking in 2015 is 18th. India fell one place (from 17th in 2013) due to its poor results in relation to promoting free trade and international standards.

Q INDIA	RESPONSE	EXPLANATORY TEXT
<b>DATA PRIVACY (SCORE: 5.6/10   RANK: 18/24)</b>		
1. Are there laws or regulations governing the collection, use, or other processing of personal information?		<p>India does not have a stand-alone data protection law, and the protections that are available are contained in a mix of statutes, rules and guidelines.</p> <p>The most prominent provisions are contained in the Information Technology Act 2000, as amended by the Information Technology Amendment Act 2008. In particular Section 43A, which addresses "reasonable security practices and procedures" and is complemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.</p> <p>However, the scope and coverage of these rules is limited:</p> <ul style="list-style-type: none"> <li>• The majority of the provisions only apply to "sensitive personal information";</li> <li>• The provisions are restricted to corporate entities undertaking the automated processing of data; and</li> <li>• Consumers are only able to take enforcement action in relation to a small subset of the provisions.</li> </ul> <p>For these reasons, India receives a "partial" result in this year's study.</p> <p>As of November 2015, a draft Right to Privacy Law 2014 law was being considered, but its progress is uncertain.</p>
2. What is the scope and coverage of privacy law?	Sectoral	The relevant provisions of the Information Technology Act 2000 (as amended) apply only to the private sector, not to government.
3. Is the privacy law compatible with the Privacy Principles in the EU Data Protection Directive?		India does not have a comprehensive privacy law. The limited provisions that are available are often unique and do not follow any international model. Some specific principles under Article 43A of the Information Technology Act 2000 can be mapped to the EU Data Protection Directive.
4. Is the privacy law compatible with the Privacy Principles in the APEC Privacy Framework?		India is not a member of APEC. The limited provisions are unique, and do not follow any international model.

Q INDIA	RESPONSE	EXPLANATORY TEXT
5. Is an independent private right of action available for breaches of data privacy?	Available	<p>The Indian Constitution does not contain a specific right to privacy, but Indian courts have interpreted some of the other provisions broadly, including the right to liberty and the right to freedom of speech. In one significant case, <i>Naz Foundation v. Government of NCT of Delhi</i> WP(C) No.7455/2001 (July 2, 2009), the Delhi High Court found a clear right to privacy did exist:</p> <p>“The right to privacy thus has been held to protect a ‘private space in which man may become and remain himself.’ The ability to do so is exercised in accordance with individual autonomy.”</p> <p>In August 2015, the Supreme Court established a special panel to determine whether the right to privacy is indeed a fundamental right of Indian citizens. This is part of an ongoing case concerning the national identity card.</p>
6. Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	Sectoral regulator	<p>India does not have a central, national regulator or complaints body for data protection (although one does exist for freedom of information).</p> <p>36 local adjudication officers operate at the state and territory levels, and these officers can receive complaints regarding breaches of the Information Technology Act. However, there are only a few reported cases relating to privacy as of November 2015 &lt;it.maharashtra.gov.in/1121/Statement-of-Cases?ID=3&gt;.</p> <p>The draft Right to Privacy Law being considered would establish a national Data Protection Authority of India (DPA).</p>
7. What is the nature of the privacy regulator?	Not applicable	<p>India does not have a central, national regulator. 36 local adjudication officers operate at the state and territory level.</p> <p>The Data Protection Authority of India (DPA), as proposed in the draft Right to Privacy Law, would consist of a chair and up to two other members.</p>
8. Are data controllers free from registration requirements?	✓	<p>India has no registration requirements for any parties under the Information Technology Act 2000.</p> <p>The draft Right to Privacy Law contains no registration requirements.</p>
9. Are cross-border transfers free from registration requirements?	✓	<p>India has no registration requirements for any parties under the Information Technology Act 2000.</p> <p>However, some rules are in place for the transfer of sensitive data offshore. It can be transferred only to a country where it is clear that the sensitive data will be adequately protected (Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules 2011). Sensitive data is defined under the 2011 rules as information relating to a data subject’s password, financial information, health, sexual orientation, medical records, and biometric information.</p> <p>Some limited restrictions on cross border data transfers are likely to be included in the draft Right to Privacy Law that is being considered.</p>
10. Is there a breach notification law?	No	<p>India does not have a data breach notification law, although significant rules and requirements are in place for general security, including mandatory compensation for security breaches that cause loss.</p>
<b>SECURITY (SCORE: 4.8/10   RANK: 17/24)</b>		
1. Is there a law or regulation that gives electronic signatures clear legal weight?	✓	<p>The Information Technology Act 2000 includes provisions that enable the use of electronic signatures in most transactions.</p> <p>Section 5 states:  “Legal recognition of digital signatures. — Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the central government.”</p>

Q INDIA	RESPONSE	EXPLANATORY TEXT
2. Are ISPs and content service providers free from mandatory filtering or censoring?	✘	<p>The Indian Computer Emergency Response Team (CERT-IN) &lt;<a href="http://www.cert-in.org.in">www.cert-in.org.in</a>&gt; was set up by the Department of Information Technology under the Information Technology Act 2000 to implement India's filtering regime. This includes administering the prohibition against publishing obscene content and the filtering of websites. CERT-IN was empowered in 2003 to review complaints and act as the sole authority for issuing blocking instructions to the Department of Telecommunications.</p> <p>In March 2015, the Supreme Court of India ruled Section 66A of the Information Technology Act 2000 unconstitutional. Section 66A imposes punishment for sending offensive messages through a communication service. Section 67 of the same act includes an offense of "publishing of information which is obscene in electronic form." This is a very broad provision as it covers "any material which is lascivious or appeals to the prurient interest." The constitutionality of Section 67 has not been questioned before the court.</p> <p>In 2011, further rules — the Information Technology (Due Diligence Observed by Intermediaries Guidelines) Rules 2011 — were introduced by the Ministry of Communications and Information Technology. They require websites to provide a response to takedown notices on objectionable content, including anything "grossly harmful" or "harassing" within 36 hours of being notified. They also require Internet service providers and social networking sites to bar certain types of content under terms-of-service agreements with users. Intermediaries are not required to act on objectionable content prior to official notification by a government authority or court.</p> <p>In May 2011, the government issued a clarifying notice relating to these rules, stating that any questions of interpretation would be resolved by the courts and not by government &lt;<a href="http://deity.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf">deity.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf</a>&gt;.</p>
3. Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	Detailed legislation	<p>The Information Technology Amendment Act 2008 includes Section 43A on "Compensation for failure to protect data," which states:</p> <p>"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource, which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected."</p>
4. Are there laws or enforceable codes containing specific security audit requirements for digital data hosting and cloud service providers?	Code of conduct	<p>Although the Information Technology Act 2000 contains a mandatory compensation requirement for security breaches, it does not contain any other requirements on security audits.</p> <p>As per the Information Technology Act, the government is required to notify / empanel a list of agencies to deal with security audits and to prescribe independent standards. However, no such notification has happened to date.</p> <p>The Data Security Council of India (DSCI) &lt;<a href="http://www.dsci.in">www.dsci.in</a>&gt;, a self-regulatory body set up by the National Association of Software and Services Companies (NASSCOM) &lt;<a href="http://www.nasscom.in">www.nasscom.in</a>&gt;, issues best-practice security guidance, but compliance is voluntary.</p>
5. Are there security laws and regulations requiring specific certifications for technology products?	Limited requirements	<p>In 2013, India was accepted as a Certificate Authorizing Member (the highest level) of the Common Criteria Recognition Agreement (CCRA) &lt;<a href="http://www.commoncriteriaportal.org">www.commoncriteriaportal.org</a>&gt;. There is growing interest in certifications in India, although no comprehensive laws or requirements are in place at this stage.</p> <p>India imposes some local security testing requirements in addition to international testing requirements. These local testing arrangements have been the subject of criticism by India's trading partners, including the European Union (EU) &lt;<a href="http://madb.europa.eu/madb/barriers_details.htm?barrier_id=115396&amp;version=3">madb.europa.eu/madb/barriers_details.htm?barrier_id=115396&amp;version=3</a>&gt;.</p>
<b>CYBERCRIME (SCORE: 7.8/10   RANK: 14/24)</b>		
1. Are cybercrime laws in place?	✔	<p>The Information Technology Act 2000 contains a range of standard computer crime provisions, many of which are applicable to cybercrimes.</p> <p>The Information Technology Act 2000 was also amended in 2008 to include a range of new more-specific cybercrime provisions. However, many of these provisions require enabling regulations before they come into force, and the relevant ones are not yet in place.</p>

Q INDIA	RESPONSE	EXPLANATORY TEXT
2. Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	✓	Although India is not a signatory to the Convention on Cybercrime, the core criminal provisions contained in the Information Technology Act 2000 closely follow the prohibitions contained in the Convention. Some provisions regarding international cooperation in investigations and enforcement that are present in the Convention are not present in Indian law. Also, requirements for data retention during an investigation that are contained in the Cybercrime Convention are also not present in Indian law. These inconsistencies do not detract from the general alignment between the Convention and the Information Technology Act.
3. What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers or other service providers?	Access with a warrant	<p>Access to encrypted data in India is subject to some limited oversight. The procedure for interception and decryption of information is set out in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.</p> <p>Under the draft Right to Privacy Law, law enforcement and intelligence services would be exempt from a large number of the privacy requirements in the law, including privacy principles for the collection and processing of personal data. It is unclear whether the draft will pass Parliament.</p> <p>In September 2015, the Department of Electronics and Information Technology released a draft National Encryption Policy. The proposed policy stated that applications using encryption would need to store plain text versions of all data for 90 days so that the content could be examined by the police if required. However, the proposal was the subject of immediate criticism and controversy and was withdrawn by the government after only a few days. The government have asked the department to develop a completely new encryption policy &lt;deity.gov.in&gt;.</p>
4. How does the law deal with extraterritorial offenses?	Comprehensive coverage	<p>Section 75 of the Information Technology Act 2000 provides that the act shall apply to an offense (under the act) or contravention of the act committed outside India if the act or conduct involves a computer, computer system or computer network located in India.</p> <p>Section 75. Act to apply to offense or contravention committed outside India:</p> <p>(1) Subject to the provisions of subsection (2), the provisions of this act shall apply also to any offense or contravention committed outside India by any person irrespective of his nationality.</p> <p>(2) For the purposes of subsection (1), this act shall apply to an offense or contravention committed outside India by any person if the act or conduct constituting the offense or contravention involves a computer, computer system or computer network located in India.</p>
<b>INTELLECTUAL PROPERTY RIGHTS (SCORE: 12.4/20   RANK: 19/24)</b>		
1. Is the country a member of the TRIPS Agreement?	✓	India became a member of the TRIPS Agreement in 1995.
2. Have IP laws been enacted to implement TRIPS?	✓	India has updated its intellectual property laws to comply with the main provisions of the TRIPS Agreement. Enforcement remains patchy in India.
3. Is the country party to the WIPO Copyright Treaty?	✗	India has not signed the WIPO Copyright Treaty. However, the 2012 amendments to Indian copyright law pave the way for India to comply with the treaty, and India may consider signing and ratifying it in the near future.
4. Have laws implementing the WIPO Copyright Treaty been enacted?	✓	The Copyright (Amendment) Act 2012 [No 27 of 2012] came into force in June 2012. It includes definitions and new provisions that help Indian law align with the treaty.
5. Are civil sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	✓	The Copyright Act 1957, as amended in 2012, contains provisions that would cover unauthorized making available of copyright holders' works online. Section 51 considers "unauthorized reproductions or communication to the public" to constitute copyright infringement. Further, Section 55 provides for civil remedies by means of an injunction, damages, accounts or otherwise in case of any copyright infringement.
6. Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	✓	Section 63 of Copyright Act 1957 provides for criminal sanctions for copyright infringements in general.

Q INDIA	RESPONSE	EXPLANATORY TEXT
7. Are there laws governing ISP liability for content that infringes copyright?	✓	<p>The Copyright (Amendment) Act 2012 [No 27 of 2012] introduces a basic Internet service provider (ISP) liability scheme, including appropriate safe harbor provisions for intermediaries that follow basic due diligence.</p> <p>Section 52(1)(c) of the Copyright Act 1957, as amended in 2012, provides a safe harbor for “transient or incidental storage of works for the purpose of providing electronic links, access or integration.” The procedure for takedown of such content is further provided for under Rule 75 of the Copyright Rules, 2013.</p> <p>Further, Clause 33.3 of the ISP License Agreement (issued by the Department of Telecom to various ISPs) requires licensees to take necessary measures to prevent any content that infringes copyright from being carried on their networks.</p> <p>In practice, the rights of copyright holders have been further strengthened by local case law (for example, Star India Pvt. Ltd v. Haneeth Ujwal (CS(OS) 2243/2014, which held that ISPs have an obligation to ensure that no violation of third-party intellectual property rights takes place through their networks).</p>
8. Is there a basis for ISPs to be held liable for content that infringes copyright found on their sites or systems?	✓	<p>Section 52(1)(c) of the Copyright Act 1957, as amended in 2012, provides a safe harbor for “transient or incidental storage of works for the purpose of providing electronic links, access or integration.” The notice and takedown procedure is provided for under Rule 75 of the Copyright Rules, 2013. Failure to comply with these provisions may attract primary or secondary liability under the Copyright Act.</p> <p>Violation of Clause 33 of the ISP License, which requires the ISP to prevent content that infringes copyright from being carried on its network, could result in termination of the ISP’s license.</p>
9. What sanctions are available for ISP liability for copyright infringing content found on their site or system?	Civil	<p>It is unlikely that criminal sanctions would apply to ISPs unless they were found to be abetting an infringement.</p> <p>However, the courts have been willing to impose civil sanctions on ISPs that do not meet their obligations to manage copyright infringements on their networks.</p> <p>In addition, violation of Clause 33 of the ISP License, which requires the ISP to prevent content that infringes copyright from being carried on its network, could result in termination of the ISP’s license.</p>
10. Must ISPs take down content that infringes copyright, upon notification by the right holder?	①	<p>Section 52(1)(c) of the Copyright Act 1957, as amended in 2012, provides a safe harbor for “transient or incidental storage of works for the purpose of providing electronic links, access or integration.”</p> <p>The takedown procedure is further elaborated under Rule 75 of the Copyright Rules, 2013, which states that the copyright owner may file a written complaint under Section 52(1)(c), on the receipt of which the person responsible for storage of the infringing copy of work is required to take steps to refrain from facilitating access to the alleged infringed copy.</p> <p>The takedown provisions are complex, and their use is not yet widespread. The law provides the intermediary with considerable discretion as to whether it is “satisfied” that an underlying copyright infringement has occurred.</p> <p>For these reasons, India receives a “partial” result in this year’s study.</p>
11. Are ISPs required to inform subscribers upon receiving a notification that the subscriber is using the ISP’s service to distribute content that infringes copyright?	①	<p>The Copyright (Amendment) Act 2012 introduces a limited notice requirement. Although there is no explicit requirement to send a notice to the subscriber, the ISP would be expected to give notice to the subscriber if it was applying the 21-day takedown action envisaged by Section 52(1)(c).</p>
12. Is there clear legal protection against misappropriation of cloud computing services, including effective enforcement?	Comprehensive protection	<p>Recent legislation in India, such as the Copyright (Amendment) Act 2012, has helped to extend Internet protocol (IP) protection to cloud services. The laws are still the subject of some confusion in India. There remain some weaknesses and gaps in both IP law and cybercrime law that may be relevant to cloud computing services.</p>
<b>SUPPORT FOR INDUSTRY LED STANDARDS &amp; INTERNATIONAL HARMONIZATION OF RULES (SCORE: 9.4/10   RANK: 11/24)</b>		
1. Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	✓	<p>Standards-setting processes in India are governed by the Bureau of Indian Standards (BIS) Act 1986 and BIS Rules 1987. Although information technology (IT) is not covered in detail in the rules, the BIS has established a comprehensive work program in relation to IT standards, managed by an Electronics and Information Technology Division Council.</p> <p>Refer to &lt;www.bis.org.in&gt;.</p>
2. Is there a regulatory body responsible for standards development for the country?	✓	<p>The Bureau of Indian Standards (BIS) &lt;www.bis.org.in&gt; has comprehensive management and regulatory responsibilities for standards setting in India.</p>



Q INDIA	RESPONSE	EXPLANATORY TEXT
3. Are e-commerce laws in place?	✓	The Information Technology Act 2000 is an omnibus law that includes provisions on e-commerce, e-signatures, cybercrime, and privacy.
4. What international instruments are the e-commerce laws based on?	UNCITRAL Model Law on E-Commerce	Parts of the Information Technology Act 2000 closely follow the UNCITRAL Model Law on E-Commerce. However, as the law is an omnibus law, it also includes a wide range of additional technology provisions.
5. Is the downloading of applications or digital data from foreign cloud service providers free from tariff or other trade barriers?	📘	No customs duty is levied on the import of software into India by electronic means. However, delivery of "off-the-shelf" software in certain physical mediums (such as installation discs) would be subject to import duties.  Note, however, that requirements relating to encryption (discussed above) may act as a potential trade barrier for some mobile applications.  India also imposes some local IT product-testing requirements in addition to international testing requirements. These local testing arrangements have been the subject of criticism by India's trading partners, including the European Union <madb.europa.eu/madb/barriers_details.htm?barrier_id=115396&version=3>.
6. Are international standards favored over domestic standards?	📘	India has traditionally prioritized compliance with international standards. However, in recent years, India has introduced additional local testing requirements for some key IT products and services.
7. Does the government participate in international standards setting process?	✓	India participates in relevant ISO and IEC standard-setting processes.
<b>PROMOTING FREE TRADE (SCORE: 5.4/10   RANK: 15/24)</b>		
1. Are there any laws or policies in place that implement technology neutrality in government?	📘	A National E-Governance Plan is in place that promotes interoperability through the establishment of common services, but it does not include a detailed commitment to technology neutrality. <www.mit.gov.in/content/national-e-governance-plan>
2. Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	📘	Although the Indian government has generally taken a technology-neutral approach, it is important to note that the 2008 amendments to the Information Technology Act included a provision that would allow the government to determine what modes of encryption companies and individuals may use:  Section 84A: "The government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption."  At the time of writing, no rules have been issued under Section 84A.
3. Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?	✗	In March 2015, the Indian government adopted a formal preference for open-source solutions for e-government procurement opportunities related to its digital agenda, the Policy on Adoption of Open Source Software for Government of India <deity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf>.  The policy states that the "government of India shall endeavour to adopt open-source software in all e-governance systems implemented by various government organizations, as a preferred option in comparison to closed source software (CSS)."  The policy applies to "all government organizations under the central governments and those state governments that choose to adopt this policy for the following categories of e-governance systems: <ul style="list-style-type: none"> <li>• All new e-governance applications and systems being considered for implementation.</li> <li>• New versions of the legacy and existing systems."</li> </ul> The policy is one of the most far-reaching and restrictive preference schemes that has been implemented to date, and is likely to have a discriminatory impact on cloud service providers.
4. Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	📘	There are multiple, complex layers of government procurement in India. Many of the state and local procurement practices give preferences to local suppliers (although these may not necessarily be relevant to cloud computing).  India is an observer, but not a member of the World Trade Organization (WTO) plurilateral Agreement on Government Procurement.

Q INDIA	RESPONSE	EXPLANATORY TEXT
<b>IT READINESS, BROADBAND DEPLOYMENT (SCORE: 10.7/30   RANK: 24/24)</b>		
1. Is there a national broadband plan?	<ul style="list-style-type: none"> <li>By 2016, fiber network to reach 250,000 local government areas.</li> </ul>	The Telecommunications Regulatory Authority of India (TRAI) <www.trai.gov.in> revisited its previous plan for the rollout of the National Optic Fiber Network (NOFN), subsequent to the release of the Digital India program in 2014 <www.digitalindia.gov.in/content/broadband-highways>. The revisited plan was addressed in detail in the report released by the Department of Telecommunication's Committee on the National Optic Fiber Network <www.dot.gov.in/reports-statistics/report-committee-nofn> in March 2015. The report details the intention to work in partnership with private organizations to build the optic fiber network, in particular, targeting nonmetropolitan communities in all states and union territories. The new timeline extended the goal to reach 250,000 local government areas (gram panchayats) by two years to 2016.
2. Are there laws or policies that regulate the establishment of different service levels for data transmission based on the nature of data transmitted?	No regulation and extensive public debate	<p>There has been considerable public debate in India on the topic of net neutrality. After campaigning from Indian telecommunication providers that were seeking government clarification and support on the issue of charging for VoIP and similar "over-the-top" (OTT) services, the Telecom Regulatory Authority of India (TRAI) &lt;www.trai.gov.in&gt; in April 2015 released a consultation paper on OTT services &lt;www.trai.gov.in/Content/ConDis/10743_0.aspx&gt;. This was followed in May 2015 by a report issued by a government telecommunications panel &lt;www.documentcloud.org/documents/2167977-net-neutrality-committee-report.html&gt;, which called for certain levels of net neutrality protections but also for VoIP calls to attract a tariff. The consultation period for this report ended in August 2015. Both of these reports received high amounts of public feedback after online media campaigns, particularly in support of net neutrality, gathered public attention. In particular, there has been strong criticism of services offering fast-lane services to paying clients.</p> <p>The Telecom Regulatory Authority of India (TRAI) released a consultation paper on differential data pricing on 10th December 2015 &lt;tra.gov.in/WriteReaddata/ConsultationPaper/Document/CP-Differential-Pricing-09122015.pdf&gt;.</p>
<b>3. Base Indicators</b>		
3.1. Population (millions) (2014)	1,252	In 2014, the population of India increased by 1.2%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/ITU-D/ict/publications/world/world.html>]
3.2. Urban Population (%) (2014)	32%	[World Bank, Data Catalog, Indicators, Urban Population (2015) <data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS>]
3.3. Number of Households (millions) (2014)	256	In 2014, the number of households in India increased by 1.2%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/ITU-D/ict/publications/world/world.html>]
3.4. Population Density (people per square km) (2014)	436	[World Bank, Data Catalog, Indicators, Population Density (2015) <data.worldbank.org/indicator/EN.POP.DNST>]
3.5. Per Capita GDP (US\$ 2014)	\$1,596	In 2014, the per capita gross domestic product (GDP) for India increased by 7.4% to US \$1,596. [World Bank, Data Catalog, Indicators: GDP per capita, current US\$ (2015) <data.worldbank.org/indicator/NY.GDP.PCAP.CD> and GDP growth, annual % (2015) <data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG>]
3.6. IT Service Exports (2014) (billions of US\$)	102.97	In 2014, the value of IT service exports for India increased by 3.8% to US \$102.97 billion. The five-year compound annual growth rate (CAGR) from 2009-2014 was 10.8%. [World Bank, Data Catalog, Indicators: ICT Service Exports US\$ (Dec 2015) <data.worldbank.org/indicator/BX.GSR.CCIS.CD>]
3.7. Personal Computers (2014) (% of households)	13%	In 2014, 13% of households in India had personal computers. This is an increase of 8.9% since 2013 and ranks India 136 out of 183 countries surveyed. The growth from 2013 is below the five-year CAGR from 2009 to 2014 of 19.5%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx>]
<b>4. IT and Network Readiness Indicators</b>		
4.1. ITU ICT Development Index (IDI) (2015) (Score is out of 10 and covers 167 countries)	2.69	India's ITU ICT Development Index (IDI) for 2015 is 2.69 (out of 10), resulting in a rank of 131 (out of 167 countries). The 2015 IDI for India increased by 6.3%, and the IDI ranking declined by two places from a rank of 129 since 2013. [International Telecommunication Union (ITU), Measuring the Information Society (Dec 2015) <www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2015.aspx>]

Q INDIA	RESPONSE	EXPLANATORY TEXT
4.2. World Economic Forum Networked Readiness Index (NRI) (2015) (Score is out of 7 and covers 143 countries)	3.73	India has a Networked Readiness Index (NRI) score of 3.73 (out of 7), resulting in a rank of 89 (out of 143 countries) and a rank of 13 (out of 36) in the lower middle income grouping of countries. The 2015 NRI for India decreased by -3% and declined from a rank of 83 since 2014.  [World Economic Forum, Global Information Technology Report (2015) <reports.weforum.org/global-information-technology-report-2015>]
4.3. International Connectivity Score (2014) (Score is out of 10 and covers 52 countries)	2.14	India has an International Connectivity Score of 2.14 (out of 10), resulting in a rank of 15 (out of 26) in the resource-driven grouping of countries.  [International Connectivity Scorecard (2013) <www.connectivityscorecard.org>]
5. Internet Users and International Bandwidth		
5.1. Internet Users (millions) (2014)	189	[International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/ITU-D/ict/publications/world/world.html>]
5.2. Internet Users as Percentage of Population (2014)	15%	In 2014, 15% of the population in India used the Internet, resulting in a ranking of 154 out of 199 countries surveyed. This represents an increase of 20% since 2013. The growth from 2013 is below the five-year CAGR from 2009-2014 of 28.1%.  [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx>]  Note: There may be some variations as to how countries calculate this. Some countries base this upon all or part of the population, such as between 16 and 72 years of age.
5.3. International Internet Bandwidth (2014) (bits per second per Internet user)	5,677	The International Internet Bandwidth (per Internet user) of India has decreased by -13% since 2013. The decrease from 2013 is below the five-year CAGR from 2009-2014 of 6.4%.  [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/ITU-D/ict/publications/world/world.html>]
5.4. International Internet Bandwidth (2014) (total gigabits per second [Gbps] per country)	1,295	India has increased its International Internet Bandwidth by 5% since 2013 to 1,295 Gbps and is ranked 28 out of 215 countries surveyed. The growth from 2013 is below the five-year CAGR from 2008-2013 of 38.5%.  [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/ITU-D/ict/publications/world/world.html>]
6. Fixed Broadband		
6.1. Fixed Broadband Subscriptions (millions) (2014)	15	India has increased the number of fixed broadband subscribers by 0% since 2013 to 15 million, and is ranked 10 out of 215 countries surveyed. The growth from 2013 is below the five-year CAGR from 2009-2014 of 22.5%.  [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/ITU-D/ict/publications/world/world.html>]
6.2. Fixed Broadband Subscriptions as % of households (2014)	6%	[International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/ITU-D/ict/publications/world/world.html>]  Note: This may be skewed by business usage in some countries.
6.3. Fixed Broadband Subscriptions as % of population (2014)	1%	India has increased its fixed broadband subscriptions (as a % of the population) by 4.2% since 2013, which is below the five-year CAGR from 2009-2014 of 13.8%. This ranks India 147 out of 215 countries surveyed.  [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) <www.itu.int/ITU-D/ict/publications/world/world.html>]
6.4. Fixed Broadband Subscriptions as % of Internet users (2014)	8%	[International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (June 2014) <www.itu.int/ITU-D/ict/publications/world/world.html>]

Q INDIA	RESPONSE	EXPLANATORY TEXT
7. Mobile Broadband		
7.1. Mobile Cellular Subscriptions (millions) (2014)	944	<p>In 2014, India increased the number of mobile cellular subscriptions by 6.5% and is ranked 2 out of 215 countries surveyed. The number of subscriptions account for 75% of the population.</p> <p>[International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) &lt;<a href="http://www.itu.int/ITU-D/ict/publications/world/world.html">www.itu.int/ITU-D/ict/publications/world/world.html</a>&gt;]</p> <p>Note: This figure may be inflated due to multiple subscriptions per head of population, but excludes dedicated mobile broadband devices (such as 3G data cards, tablets, etc.).</p>
7.2. Active Mobile Broadband Subscriptions per 100 inhabitants (2014)	6	<p>India has increased the number of active mobile-broadband subscriptions (as a % of the population) by 72% since 2013. This ranks India 162 out of 215 countries surveyed.</p> <p>[International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) &lt;<a href="http://www.itu.int/ITU-D/ict/publications/world/world.html">www.itu.int/ITU-D/ict/publications/world/world.html</a>&gt;]</p> <p>Note: This refers to the sum of standard mobile-broadband and dedicated mobile-broadband subscriptions to the public Internet. It covers actual subscribers, not potential subscribers, even though the latter may have broadband-enabled handsets.</p>
7.3. Number of Active Mobile Broadband Subscriptions (millions) (2014)	70	<p>In 2014, India increased the number of active mobile-broadband subscriptions by 74% and is ranked 7 out of 215.</p> <p>[International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2015) &lt;<a href="http://www.itu.int/ITU-D/ict/publications/world/world.html">www.itu.int/ITU-D/ict/publications/world/world.html</a>&gt;]</p>