DEEPSTRAT
STRATEGY . POLICY . ACTION

C4CII: Cloud for Critical Information Infrastructure

Anand V., Shachi S., Gauri S. K.

DEEPSTRAT

STRATEGY . POLICY . ACTION

About DeepStrat

DeepStrat was founded with the vision to combine the rich experience of its founders to deliver sustainable solutions. We help our clients scope, design and implement their strategic goals through custom-made solutions, guided by cutting-edge research.

We offer our unmatched experience, deep networks and a multi-disciplinary research expertise to deliver the mandates of our partners and clients. The DeepStrat network offers decades of experience in risk assessments and management, public policy, regulatory, compliance and tax advisory, crisis management, research, and strategic communications across Asia.

If you are looking to partner with us, drop us an email at contact@deepstrat.in.

About the Authors

Anand Venkatanarayanan is co-founder and Chief Technology Officer, DeepStrat.

Shachi Solanki is Deputy Chief of Operations and Lead, Policy Risks Vertical, DeepStrat.

Gauri S. Kumar is Senior Programme Associate, DeepStrat.

Designed by

Shriya Bhatia, Lead Graphic Designer, DeepStrat.

Suggested citation:

(C4CII:Cloud for Critical Information Infrastructure; Anand V, Shachi Solanki and Gauri S Kumar; DeepStrat, 2023)

This report is also available on https://deepstrat.in/all-articles/

Acknowledgements

This report wouldn’t have been possible without the valuable assistance, guidance and time that a number of experts willingly gave us. A number of senior officials from the Reserve Bank of India generously gave time to share their views and inputs on how they perceive the use of cloud services in the BFSI sector. From the power sector we had a few experts sharing their expertise, and most notably, Mr Anil Kumar Sharma of Dakshin Haryana Bijli Vitaran Nigam (DHBVN), one of the main Discoms of Haryana. We also received feedback from Mr Akash Mahajan and Mr Riyaz Walikar, Co-Founders of Kloudle Inc. whose inputs were very insightful and helped us understand how to manage security for cloud services. We are also grateful to Mr Pradyot Choudhary, COO, Aarvy Hospital, who graciously shared his insights on the use of cloud in the health sector. Mr S N Panda, former Chief General Manager, RBI was forthcoming and a valuable guide for this report. Finally, while this study was enabled by the expertise of many, any mistakes that may have crept in are purely our own.

Contents

Executive Summary

The era of digitisation may have begun, when the Personal computer became available as a mass market device in the year 1970, when the Altair 8800 was introduced, but it accelerated at great speed in the 2000s, when internet companies figured out how to create ware-house sized giant computers, by networking cheaper desktop computers and inventing the first "Proto Data Centre OS", which operates all computing, storage and network assets in a data center, as one single unit, with physical partitions that provide resiliency against failures.

While the construct of Critical Information Infrastructure (CII) existed even before this, the invention of Ware-house sized computers, which heralded the Cloud computing era, brought forth changes in not how CII was defined and understood, but also guidelines around how these systems were secured, managed, and mitigated against a range of risks.

This report analyses these controls across multiple jurisdictions and verticals from multiple perspectives (IT Security Practitioners, Regulators, Auditors, Executives, Board Members), with a specific focus on the guidelines notified by National Critical Information Infrastructure Protection Centre (NCIIPC), the nodal agency responsible for protection of CII in India.

It also attempts to answer the following questions:

Q1. **How is cloud adoption viewed within current (and potential) CII entities in their digitisation journey?**

While most sectors within the CII sectors are still evaluating using Public Cloud for their needs, there is a general hesitancy in migrating towards public cloud because of data security concerns and lack of guidance from the regulators. The hesitancy is most pronounced in Transport, Strategic and Health sectors, while the financial sector has been leading in Cloud adoption, because of clear principle-based guidelines from the sectoral Regulator (RBI).

Q2. **How do Cloud services measure up to the scale and cyber security requirements for entities notified (or in the process of being notified) as CII, against the NCIIPC guidelines?**

The controls notified by NCIIPC can be fully implemented using service offerings provided by all the major cloud service providers. However, there are several controls that are very generic in nature and need to evolve and be refined further if they must be relevant.

Q3. **What should policymakers consider when drafting regulations as part of the overhauling of the IT Act, when it comes to entities under the CII framework?**

NCIIPC Guidelines need to be revised

With the last update to the Guidelines made in 2015, eight years is a long time in the Cyber Security industry for a guideline to remain relevant. As the technical analysis of these guidelines indicate, it is not possible to evaluate the implementation applicability of many controls, as they are either too generic or not relevant, even by security practitioners. A comparative analysis of other jurisdictions reveal that standards are updated at a 2-to-3-year cadence, at the very least.

The guidelines must not only be revised, but it should also add implementation guidance for entities, on Cloud adoption, as the entire ecosystem (CI Entities, Auditors) struggles to adapt to the guidelines in practice.

Cloud Security Regulatory Framework Should Be Harmonised

A cross sectoral analysis of regulatory framework on cloud security shows that there are three different approaches adopted by the regulators:

- Controls based - The NCIIPC guidelines.
- Principle based – The RBI Master directions on IT Outsourcing.
- Principle based – SEBI Framework for Adoption of Cloud Services.

Furthermore, there is also deviation in the standards that entities must adopt to. For instance, none of the SEBI, RBI and NCIIPC frameworks specify the standards for entities to follow, but the IT Rules indicate it should be ISO 27001 based. This leads to severe confusion for the entities, boards, and auditors on how to go about implementing controls and auditing them, as there is no way to harmonise practice on differing philosophies and lack of standards.

Internationally, however there is an effort towards defining standards first, and then an overarching principle-based approach, with sectoral regulators fine tuning guidelines within the larger ambit of standards and principle in consultation with Cloud Service Providers and Entities, with extensive guidance on implementing those, via risk assessment frameworks.

A shift towards this approach would reduce the compliance burden on CI entities, which might end up under different sectoral regulators and improve their cybersecurity posture.

Adopt Data classification for impact and risk assessment

While the controls-based approach forms the basis for the NCIIPC guidelines, it is at the other end of the spectrum compared to the principle-based approach taken by the RBI. Critical sector entities however require specific guidance from the regulators on moving their workloads to the cloud and a risk-based approach that identifies workloads based on data classification and impact (Low, Moderate, High) based on NIST standards (FIPS 200, March 2006) would be a middle path to take, while revising the controls-based approach and harmonisation of regulatory framework.

Consultation should be an integral part of rule making

The nature of the Cyber domain is that rule making cannot be divorced from implementation. With rapid digitisation, attack surfaces have increased exponentially. Hence check box approaches do not work and only create a sense of false security. Policy makers hence need to avoid suggesting prescriptive approaches and evaluate new models and frameworks based on evolving risks.

These models cannot however be evolved without extensive consultations with all parties concerned including CI entities, CSPs, Auditors, Standard bodies and other interested parties including Civil society organisations.

Capacity Building

Policy should acknowledge that CII entities will continue to use public cloud for various purposes, and provide enough guidance to those who chose this path, and should include:

- Pilot Projects, sandbox approach to build confidence for entities to experiment with cloud.
- Technical skilling of IT teams in emerging technologies and cyber security to bridge knowledge gaps.
- Training for auditors in the cloud environment to address capacity constraints in the auditing field.

1 Introduction

The Information Technology Act, 2000 is the overarching legislation for all matters pertaining to digital infrastructure in India. In 2008[1], it witnessed a major amendment aimed at enhancing the cybersecurity of the country. The amendment brought about a new definition of "Critical Information Infrastructure"[2] (CII) and created a nodal agency—the National Critical Information Infrastructure Protection Centre (NCIIPC)—for its protection under Section 70A of the Act.

The operating Rules notified in 2013[3], defined the charter for NCIIPC, which includes identification of CII elements, advising on reduction of vulnerabilities, and providing strategic leadership and coherence across government for responding to cybersecurity threats against CII. For fulfilling its role, as per these rules, NCIIPC has laid down guidelines, which cover identification and notification of entities as CII based on several criteria[4] . These entities are expected to implement a set of 40 controls, under buckets such as Planning, Implementation, Operational, Disaster recovery / Business Continuity.

The Government is planning to overhaul the IT Act, 2000 with a comprehensive Digital India Act and prescribe governing provisions for emerging technologies[5]. Given that the NCIIPC guidelines were notified in 2013, and the fact that the world-wide annual spending on Cloud Services has increased from approximately $10B to $100B[6] during that time, the following questions arise:

Q1. How is cloud adoption viewed within current (and potential) CII entities in their digitisation journey?

Q2. How do Cloud services measure up to the scale and cyber security requirements for entities notified (or in the process of being notified) as CII, against the NCIIPC guidelines?

Q3. What should policymakers consider when drafting regulations as part of the overhauling of the IT act, when it comes to entities under the CII framework?

This report attempts to answer the above questions through primary and secondary research and analysis, interviews with industry practitioners, regulators, auditors, and executives responsible for security operations across various entities notified under the CII regulations. The report has six sections:

1. **Background on CII** – It traces the historical evolution of the CII Sector to the writings of Austrian war strategist Carl Von Clausewitz and his formulations on Center of Gravity and Critical Vulnerabilities. The historical context situates the CII definition, which while flexible and variable across jurisdictions, is trending towards a practical definition of 'Any service that has adoption over a threshold is a potential CII'.
2. **Technical Evaluation of NCIIPC guidelines** – It explores how cloud computing evolved from the unique needs of giant internet companies, which created a technical architecture of networking millions of desktop computers to create giant warehouse scaled computers, to provide resilience, scale, and performance for their numerous services, which were then offered to enterprise users

[1] (Ministry of Law and Justice, 2009)

[2] The Act defines "Critical Information Infrastructure" to mean "any computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health, or safety.

[3] (Ministry of Electronics and Information Technology, 2014)

[4] (NCIIPC, 2015, p. 5)

[5] (Barik, 2022)

[6] (Synergy Research, 2020)

as Cloud Services. Further, the chapter does a technical evaluation if the existing CII regulations in India could be met by cloud and points out areas where regulations need to evolve.

3. **Regulatory Analysis of global CII regimes** – This section performs a legal analysis of CII regulations from other Countries (US, Singapore, Australia, Germany and Japan). It then delves into how they have dealt with Cloud Adoption and the relative merits of the same.
4. **Regulatory Analysis of NCIIPC guidelines** – It details the doctrinal approach of NCIIPC and does a comparative study with that of US, Singapore, Australia, Germany and Japan.
5. **Insights from Interviews –** The section explores views of various stakeholders on CII regulations, Cloud Security, and their plans to migrate their workloads to Cloud.
6. **Recommendations –** This section makes a set of recommendations that policy makers must consider, to make the CII regulations more relevant and useful for entities that are considering Cloud adoption.

2 Backgroud on CII

The historical construct of Critical Information Infrastructure is drawn from celebrated Austrian war strategist Carl von Clausewitz's book, *On War* in which he often used the term Centre of Gravity (COG) to define a "concentration of mass," in both offensive and defensive terms. "*It presents the most effective target for a blow; furthermore, the heaviest blow is that struck by the centre of gravity.*"

Acknowledging that generals in the history of warfare had used this rationale, he wrote that war planning was thus "*a major act of strategic judgment to distinguish these centres of gravity in the enemy's forces and to identify their spheres of effectiveness*". The dual reference to Center of Gravity in both offensive and defensive terms led to some confusion. Strategists grappled with the conundrum whether a Center of Gravity is also a Critical Vulnerability.For example, The US Navy war fighting manual[7] posited that "*Applying the term to modern warfare, we must make it clear that by the enemy's centre of gravity we do not mean a source of strength, but rather a critical vulnerability.*"

Strange[8] then cleared the confusion, and introduced the construct of CG-CC-CR-CV as below:

- CG - Center of Gravity
- CC - Critical Capabilities (abilities which can identify a CG)
- CR – Critical Requirements (conditions required for a critical capability to be operational)
- CV – Critical Vulnerabilities (requirements which are vulnerable to neutralisation)

The US Presidential Decision Directive 63 (PDD-63)[9] was the first policy guidance on critical infrastructure (CI) protection for both physical and cyber, in the modern era. Its framing of the term "Critical Infrastructure" was closer to the elimination of Critical Vulnerabilities, than to that of a Centre of Gravity (CG). The directive focused on defending critical infrastructure is essential for preserving national power against potentially devastating asymmetric attacks, and identified several key elements to implement the directive, including public-private partnerships, organisation structure, lead agencies, sectoral co-ordinators and even low-level tasks that need to be completed within 180 days.

Considering that establishing the criterion for assessing criticality depends on numerous factors including the perceptions of those making the assessment[10], it was a hard problem to be done within 180 days.

The Evolution of CII

As digitisation grew in the 2000s, more industries and sectors which were isolated in physical space became more interconnected in cyber-space. This trend changed the conceptual definition of CI—evolving from avoiding catastrophic events to avoiding and mitigating disruptive events for enabling prosperity, public safety, and a comfortable civic life.

> For instance, Australia, Canada, New Zealand, United Kingdom, and the United States share a common definition of Critical Infrastructure as: *"Critical infrastructure, also referred to as nationally significant infrastructure, can be broadly defined as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations"*[11]

[7] (US Marine Cops, 1989, p. 85)

[8] (Joe, 1996, p. 2)

[9] (The White House, 1998)

[10] (Humphreys, 2019, p. 1)

[11] (CISA, 2014)

As the Organisation for Economic Cooperation and Development (OECD) report notes, CII definitions range from societal well-being to nation state security concerns and the flexibility allows individual states to better address their risk in a dynamic environment without becoming too prescriptive.

The Information Technology Act of 2000 was a statutory effort to protect India's growing service industry in the Information Technology Enabled Services (ITES) sector but did not recognise cybersecurity. In 2008, the Government of India amended the IT Act of 2000 to define cybersecurity as" protecting *information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification, or destruction*". The new Act further than defined CII as: "***Critical Information Infrastructure*** *means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.*"

Globally, a side effect of this flexibility in CII definition is the expansion of CII tag to more sectors and industries. While there are common sectors, such as Energy, Finance, Transport, Water and Core Information and Communication, the list can be variable because of the definitions that each country follows. As the definitions can be dynamic, the sectors identified as CII also change over time.

The CII tag also depends upon the Cyber Security doctrine of a particular nation state. For instance, the Russian information security doctrine[12] views national security through the prism of information security including influence, erosion of traditional moral and spiritual values, and hence views CII as 'Unified State System' run by the Federal Security Service (FSB)[13]. This approach is different from the traditional approach where CII is often owned by the private sector and regulations push for voluntary participation by declaring standards and encouraging data sharing via specialised entities.

The Chinese CI definition includes not just the traditional sectors but also e-commerce websites and social media[14].

One emerging trend from the above examples is that any service that has a concentration of people (adoption) beyond a certain threshold becomes a Center of Gravity, with concentrated mass (Classic Clausewitz definition) and hence becomes a potential candidate for a CII tag.

CII Risk Management

The criteria for identifying CII are dynamic, and the bureaucracy and tools deployed to protect CII systems vary across nation states. This is because in the cyber domain defense is not only technical but is organisational and involves prioritisation of resources and maybe subject to inter-departmental wrangling on both private and public sectors. There are four problems that keep repeating in managing risk for CI Systems [15] [16]:

1. Private sector ownership: Most of the CII systems will always be owned by the private sector, which individually may not possess the ability to see the big picture, as a nation state CI regulator would. Private CII entities on their own might not have the budgets or resources required to fend off dedicated nation state adversaries and hence need state power and resources to shore up their defences. CI regulators, however, need data (both technical and operational) from CI operators to

[12] (Russian Federation, 2016)

[13] (Pursiainen, 2020)

[14] (Jong-Chen & Brian, 2017)

[15] (Humphreys, 2019, pp. 11 - 26)

[16] (OECD, 2019)

determine emerging threats, but may most often not share data about these threats to CI operators for several reasons, including lack of trust.

2. Blindsiding expertise development: The nature of the Cyber domain and the upward trend of digitisation implies, there are always blind spots within the CII operators' systems, which leads to inevitable public incidents. In the aftermath of these public incidents, regulators typically over-react and push for prescriptive mandates, which may focus on pushing processes that are designed to thwart a repeat of the public incident and may fall short of developing the expertise to identify and thwart emerging threats, which is the larger purpose of the regulator.

3. Greater focus on offensive operations/ Lack of incentives for private sector participation in CI ecosystem building: Cyber defense and offence are two sides of the same coin as the defensive techniques evolve based on discovered offensive operations and vice versa. Typically, CII regulators start off as a part of the organisation that does offensive operations[17]. However, soon this becomes an issue of focus and budgets. The CII regulator may eventually get into conflict with multiple other government organisations as the definition of CII undergoes change and eventually comes under the department(s) that handle internal security, which emphasise mandate -based prescriptive approaches, while ignoring capacity issues and the for-profit nature of the CI operators. This creates strong dis-incentives for an operator to become part of the CI ecosystem, as they perceive it as an impediment to their core business without any tangible benefit[18].

4. Fragmentation of processes: CII regulators often do sectoral classification and go about creating regulators and coordinators at a sectoral, state (county) and national level (See Humphreys, 2019 Page 22 for a detailed discussion on this). This approach creates fragmentation of processes that need to be followed by CI Operators which reduces effectiveness of risk management. Inevitably this leads to more conceptual questions of risk management and rise of other frameworks[19].

Managing CII risk, as the above repeating patterns indicate, belongs to a class of problems called "Wicked Problem," as the stakeholders (CI Regulators and Operators) have vastly different world views, which are often irreconcilable, but both stakeholders are expected to work together and take shared responsibility. CII regulators and operators have enhanced apprehension because of national security and geopolitical concerns, which makes their relationship more complex than the usual stress that exists between regulator and regulated entities. Research indicates that this is a "Type 3" [20] wicked problem because of a difference in the problem statement and the solution and hence, collaborative strategies would yield more success than competitive or authoritative strategies.

The Rise of Public Cloud & CII

CII was already a complex concept with variable definitions and dealt with a multitude of sectors, technologies, requirements, laws, regulations as well as socio-political constructs. Into this

[17] For instance, NCIIPC is part of the National Technical Research Organisation (NTRO), which is responsible for offensive operations.

[18] (OECD, 2019, pp. Chapter 3, Last Paragraph)

[19] (OECD, 2019, p. Chapter 5) explains this as "The diversity and complexity of shock events, the increased interdependences and interconnectedness, climate change, the fast pace of innovation that fundamentally transforms critical infrastructure sectors, as well as ageing infrastructure, are among the challenges with which critical infrastructure resilience policies must contend. Many researchers on this topic conclude that a shift in focus from **protection to resilience** would help policymakers to better account for uncertainty."

[20] (Roberts, 2017, pp. 3 - 7)

complexity arrived recent technologies such as Cloud Computing, which brought efficiency and disruption in equal measure. It introduced quite a different approach to computing and cybersecurity (discussed in depth in the next chapter), with innovation that prioritised agility of development, elasticity of resource management and pricing such as the pay-as-you-go model [21].

It was inevitable that at some point, CII operators would want to leverage the benefits of cloud and Operators seeking efficiency, were now following this trend to Cloud Service Providers (CSPs). They however, had to contend with another challenge - To move towards CSPs needed a move towards a shared responsibility model, from their existing comfort level with fully on-premises hardware (which are sometimes cut off from the internet), on which they alone have full control.

While the existing relationship between CII operators and regulators was already complex, the rise of public cloud has brought forth more complexity into this wicked problem. It is inevitable that some of the potential CI entities would have heavily invested in building a cloud strategy when they were not yet Centres of Gravity. As public cloud works on a shared responsibility model between the operating entity and the CSP, when the entity becomes critical enough to earn the CII tag, CSPs become another stakeholder in this process.

From a policy making perspective, this opens several questions including prescriptive vs performance-based approaches. CSPs may also have to convince governments/regulators that they have robust safeguards against unauthorised access to sensitive data and that their services are provided from data centres located within the geographic boundaries of the home country. This makes them an interested party in not just the standard setting process of CI risk mitigation. Devoid of hard power, they would always prefer the collaborative incremental approach, while states may choose an authoritative strategy, which could erode the trust between CI operators and Cloud Service providers.

[21] (Synergy Research, 2020)

3 Technical Evaluation of NCIIPC Guidelines

Evolution of Cloud Security Model

While it may be easier to think of Cloud Security model as a set of principles[22] from an operational perspective, this approach does not capture the trends and themes that led to the rise of cloud computing. Cloud evolved from specific needs of companies that were forced to innovate to offer internet-scale performance, networked together to behave like one computer across the entire data center, sometimes referred to as Ware-house scale Computer (WSC) [23] offering economies of scale.

The scalability of cloud therefore consists of multiple other sub-problems:

1. Is the compute (CPU) scalable?
2. Is the network scalable?
3. Is the storage scalable?
4. Is the orchestrator that controls the above (Control Plane) scalable?

In the initial days of WSC, Scalability was typically achieved by treating all applications and services as a set of jobs[24], which then executed in a cell (a set of computers managed as a unit). While this approach was sufficient to manage the requirements, there were few issues:

- Using jobs only as a grouping mechanism is overly restrictive.
- One IP per machine complicates port allocation.

An important learning from WSC is - Cluster Manager, which manages job allocation, execution, tracing, resource allocation etc. in a set of networked computers is the "**Kernel of a Distributed System.**"

While in a desktop computer or a server, the Operating System manages processes, created by several users, and enforces resource constraints, isolation and reclamation, the Cluster manager performs similar functions, with the following differences:

- It manages several thousand computers, instead of a single computer.
- The processes are not just long running or ephemeral jobs but could be a wide variety of workloads such as Virtual Machines, Docker Containers from multiple users across different organisations and other internal processes (agents, services) that perform the essential functions of the Cluster Manager.

One interesting side effect of running a multitude of workloads in Cloud is that it forces the providers to go down the stack. While in the initial days, Cluster managers were built on top of existing Operating systems like Linux (or their distributions such as Ubuntu, Red Hat etc.) and Windows, the quest to squeeze out more performance and improve security, made them invest in building their own custom OS (e.g., Amazon Linux, Google Container Optimised OS) and Hypervisors (e.g., Amazon Nitro, Azure Hyper-V, Google KVM). Providers eventually ended up building their own Chips for custom workloads (e.g., Google Tensor Processing Units, Google Tau T2A for ARM, Amazon Graviton for ARM, Alibaba Yitian for ARM).

Thus, it might be better to think of Cloud as not a set of services or as service models such as Infrastructure as A Service (IaaS) or Platform as A Service (PaaS), but as a "Proto Data Center OS"[25] in making, which will eventually contain a full vertical stack from Silicon (CPU, TPU, ASIC), Hypervisors, OS, Networking Layer, Storage Services and more. The "Proto Data Center OS" operates all computing, storage and network assets

[22] (Center, National Cyber Security, 2018)

[23] (Barroso & Hölzle, 2009)

[24] (Verma, Pedrosa, Korupolu, & Oppenheimer, 2015)

[25] (Flake, 2020)

in a data center, as one single unit, with physical partitions that provide resiliency against failures (referred to as availability zones). Scalability and performance hence are first order constructs in the Cloud and are not bolted-in later.

Practitioners[26] reiterate this aspect by pointing out that *"When people got stuck with scale in terms of ceiling of performance, they migrated to the cloud, simply because there were more options. And because of the marketplace model, there are a lot easier security solutions to be bought. And whenever they wanted performance, and to cater to the kind of engineers they would be able to hire, they all move to cloud."*

A key aspect in Cloud is programmability. Everything from compute, network and storage is available via APIs, which should allow anyone with a credit card to create a miniature WSC environment for themselves. The API based approach allows automation at scale, where entire environments can be built, configured, modified, and can be torn down via single commands with reproducibility[27], thus bringing down time to market for developing a new product, at minimal cost (because of the pay-as-you-go model).

The fundamental construct through which users view the Cloud Security model is via Accounts and Organisations. A Cloud Account is a sandbox within which all the user created cloud resources like (Networks, Storage, Virtual Machines, Services). This sandbox is not accessible to other users (Accounts) unless made available through policies enforced by an Identity and Access Management (IAM) layer that the cloud user decides. This is distinct from accessing the resources from the internet, which are managed through a series of network policies, load balancers and DNS addresses. The user has full control over who can access what resource and in what capacity. The IAM layer and policy-based access to resources through programmatic APIs is an essential aspect of Cloud security model (like how user access control is an essential element in a typical Multi-user OS).

Accounts are a handy way to sandbox not only a given "user" but also environments like Development, Production, and Staging. Hence a typical Cloud user has the option of opening several accounts and linking all of them as belonging to a Single Organisation, for not just billing and management purposes, but also to limit blast radius in the case of a breach [28] [29]. Cloud Service Providers thus provide a way to organise accounts linked to an organisation (Legal entity) via hierarchical management groups, which not only mimic internal organisation structure, but also provide better compliance controls.

An efficient way to manage the security complexity of a "Proto Data Center OS" is abstracting out several hundred thousand of networked computers across data centers, acting as a single computer in which workloads[30] from several thousands of organisations, each of which, may have several accounts is via the Shared responsibility model. In this model, Cloud Security is divided into two distinct concepts:

[26] Akash Mahajan and Riyaz Walikar, Co-Founders of Kloudle Inc. The term practitioners in this section, would always be used to refer to validated interview quotes from them, in this section.

[27] For more information on how this could be done, consult documentation on popular tools like Terraform, Pulumi, CDF Kit, Chef, Puppet, Ansible etc.

[28] (Amazon Web Services, 2021) provides a detailed reference on why multiple cloud accounts for a single organisation is a good security practice.

[29] (Microsoft Azure, 2023) deals with multiple cloud accounts as a subscription and resource management problem, using resource groups.

[30] The term workload refers to any Computing, networking or storage service that can be run on a Cloud including Virtual Machines, Databases, Neural Networks etc.

1. Security of the Cloud (Responsibility of the CSP) – Protecting the hardware, software and services that make the Cloud, i.e., Security of the Data Center OS.

2. Security in the Cloud (Responsibility of the User) – Configuring, Managing, and deploying a given workload that a user chooses to run in the Cloud, using the security controls given by the Cloud Provider, i.e., Security of the Individual workloads that run in the Cloud.

This is like how Single Computer OS approaches security controls. The security of Kernel, Device Drivers and various System services that together form the OS is the responsibility of the OS Vendor, while the security of applications that are run by various users, is the responsibility of the users.

Cloud as a Single computer being run by a Proto-Data Center OS, provides a robust conceptual model for evaluation of various regulatory frameworks that govern the CII sector, because in a way, the regulatory framework dictates the boundary between the OS and the applications. If the regulations are too prescriptive, they may end up distorting the security boundary evolved over a decade of deploying several million different workloads and hence may create a net negative effect. On the other hand, if they are too generic, they may not provide enough guidance for CII operators (both current and future) to securely move their workloads into public cloud.

One way to evaluate if the existing CII regulations in India could be met by the Cloud providers is to do a gap (technical) analysis of these regulations against the known capabilities of the providers and note down the areas, where the regulations are too prescriptive or generic.

NCIIPC Guidelines for Protection of CII

Entities identified by NCIIPC are expected to implement a set of 35 controls[31], under buckets such as Planning, Implementation, Operational, Disaster recovery / Business Continuity. The methodology used to analyse if Cloud Services can be used to implement these controls is described below:

- Every control is first categorised as technical, organisational or a mix of both.
- If a control is purely organisational or if it is too generic technically, then analysis of the control is skipped.
- If controls are like one another, they are clubbed together for the analysis.
- Technical controls are then evaluated against the capabilities of the major cloud providers (AWS (Amazon Web Services), Microsoft Azure, Google Cloud) on three parameters – Relevance, Cost and Support level, with a summary note on implementation, which is then validated with practitioners.

The table below categorises controls and records those which are skipped.

[31] (NCIIPC, 2015)

Type	Controls Analysed	Controls Skipped
Planning	• PC2: Vertical and Horizontal Interdependencies	• PC1: Identification of CII • PC3: Information Security Department • PC4: Information Security Policy • PC5: Integration Control • PC6: VTR Assessment and Mitigation Controls • PC7: Security Architecture Controls including configuration Management and Mitigation Controls • PC8: Redundancy Controls • PC9: Legacy System Integration • PC10: Supply Chain Management – NDA's, Extensions and Applicability • PC11: Security Certifications • PC12: Physical Security Controls
Implementation	• IC1: Asset and Inventory Control • IC2: Access Control Policies • IC3: Identification and Authentication Control • IC4: Perimeter Protection • IC5: Physical and Environmental Security • IC6: Testing and Evaluation of Hardware and Software	None
Operational	• OC1: Data storage: Hashing and Encryption • OC2: Incident Management Response • OC4: Data Loss Prevention • OC6: Asset and Inventory Management • OC7: Network Device Protection • OC9: Critical Information Disposal and Transfer	• OC3: Training, Awareness and Skill up-gradation. • OC5: Penetration Testing • OC8: Cloud Protection • OC10: Intranet Security • OC11: APT protection
DR/BCP	• DR1: Contingency Planning – Graceful degradation. • DR2: Data Back-up and Recovery Plan, Disaster Recovery Site • DR3: Secure and Resilient Architecture Deployment	None
Reporting / Accountability	None	• RA1: Mechanism for threat reporting to Govt. Agencies • RA2: Periodic Audit and Vulnerability assessment • RA3: Compliance of Security Recommendation.

IC (Implementation Control) 1: Asset and Inventory Control

PC2: Vertical and Horizontal Interdependencies

OC 6: Asset and Inventory Management

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Yes
Cost	Nil (Enumeration APIs are in the CSP Control Plane and hence do not incur additional charges)

Asset and inventory management in Cloud is a far easier problem than managing on-premises hardware resources, which require tagging and movement control registers. There are two reasons for this simplicity:

1. All the Assets in the Cloud are created using orchestration tools. Further, even when the resources are created by other means, it is trivial to enumerate the existing resources through these APIs. Software tools that can do this, while only requiring limited permissions to do so[32].
2. Unlike Hardware assets that require tagging w/ stickers/RFIDs, asset tagging in Cloud is accomplished via Tagging APIs, which allow adding any tags to any resource. Software tags using key value pairs are in theory unlimited and propagate across resources created by templates. Further permissions on these resources can be based on these tags. Policies are often written using conditionals based on these tags.

Software asset management however could be as effort-intensive as in the case of On-premises model that CII systems traditionally rely on. This is because software dependency management is always a complex problem and creating a BOM (Bill of Materials) is of limited help[33]. While cloud native tools such as AWS Fleet Manager, Azure Operations manager, and other tools such as Chef, Puppet, Ansible mitigate the problem, they do not fully solve it, as it is a multi-dimensional matrix across various deployment models (VM Images, OSes, Patch Versions, Docker Images, Cloud Functions.

Tags also aid in understanding dependencies between internal and external organisations, as it is customary practice to add department and billing information while tagging the resources. When combined with visualisation tools, it makes analysing dependencies much easier.

Practitioners however note that *"It is no different from how it would be done in a data centre. There is no difference, because the same networking, which would have allowed multiple servers to have multiple different versions of operating system and software to be installed in a data centre, the same is available in the cloud. Right at that layer, it makes no difference. But because of the capability to execute commands, with the right access, and permissions, it is possible to build the bill of material or software inventory continuously, or even like start from where only this software should be present in this kind of hardware. All of that is very, very easily done in the cloud, because of the API's provided, and the nature of how everything is software defined."*

They further note that *"Because of the shared responsibility model of all cloud providers, if there is a service whose patch management and responsibility of the software version is on the cloud provider,*

[32] For non-exhaustive list of such tools for AWS (https://github.com/toniblyx/my-arsenal-of-aws-security-tools), Azure https://github.com/kmcquade/awesome-azure-security.

[33] An informal discussion about SBOMs and why several assumptions about them do not hold, see SBOMs and Jelly Fish by Dave Aitel (https://seclists.org/dailydave/2022/q2/0)

then they automatically take care of ensuring that they are upgraded to a particular version. And continuous information is being shared by the top products used by the customer."

IC 2,3: Access Control Policies and Identification and Authentication Control

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Yes
Cost	Nil (for baseline controls, while advanced controls may incur additional charges)

Access control to any cloud resource is typically implemented through the IAM (Identity and Access Management) layer with the following constructs:

Identity – Identity is managed through users, groups, and service principals. Users and Groups can be natively created or synchronised through third party Identity providers via LDAP, Active Directory, SAML, OAUTH protocols, like how an OS supports pluggable authentication methods (PAM). By default, any given identity has no access to any resources.

Policies - Policies determine access to a resource by a given identity. This is done either by attaching the policy to an identity directly or creating a role and attaching it to an identity, that allows or denies any given action, on a set of resources. As they are defined and declared through a domain specific language (XML, JSON), policies can also embed conditionals, and can support a wide variety of logical operations to implement any type of access control that is relevant to the organisation.

Monitoring – Cloud providers by default, support logging of all identity and access control events and make it available as a log stream. The stream can be ingested into either native log analysis services or third-party logging services for actionable insights. When coupled with serverless resources (e.g., AWS Lambda, Azure Functions), it is possible to create automated mitigation actions (e.g., Block access after "n" failure attempts) with very minimal costs.

Practitioners point out that "*Amazon Web Services, Google Cloud, Microsoft Azure are these three big ones that we actively work with. IAM is a separate service that they provide. And the best part about this service is it runs independent of all the compute all the servers that you have, which means that even if a server is compromised, your IAM is not. So, in the cloud world, even Windows servers are far safer because there is no physical access by default. And to get control access, or even remote access, you must explicitly allow it. So, it is possible to build the exact kind of elevated access control process you would want, which was theoretical in the past, because there was like a physical machine involved, which could be stolen. But it is much easier to do so in the cloud.*"

IC 4: Perimeter Protection

OC 7: Network Device Protection

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Yes
Cost	Nil (for baseline controls, while advanced controls may incur additional charges)

Virtual Private Clouds (VPC) are like traditional networks in a data center and provide logical isolation for all resources. Perimeter protection is provided by an entire range of constructs such as:

Subnets: A VPC can have several subnets within its network range. Each of these could either be private or public, which determines if they are accessible through the internet. While public subnets are typically attached to an internet gateway, private subnets are not and are only accessible through IAM via native tools (Azure Bastion, AWS System Manager)[34]. For Virtual machines, that only need to access internet, Network Address Translation (NAT) Gateways are a good option.

Security groups and Network ACLs: Individual Virtual machine can be segmented through security groups (which define lists for ingress/egress), while network segmentation can be achieved via Access Control lists (that support both allow/deny lists)[35].

Network Traffic Monitoring[36]: Traffic monitoring is supported through flow logs, which can be enabled at a VPC level or subnet level or individual security groups. The logs can be ingested into native log analyser services or through external services for high level analysis and automated actions.

Firewall: Both Native and external firewall solutions exist (which can scale seamlessly) and can block traffic (for entire VPCs (Virtual Private Cloud), subnets or individual VMs) using rule sets. The rule sets can be pre-defined by the cloud provider or could be custom, based on threat feeds and can be mixed and matched, to support any requirement.

Practitioners also point out that *"The network is now more context aware in the cloud with policies like conditional access, which has led to the emergence of security tooling and products, which scale very well as they can check for billion attacks per day, as they're able to combine the intelligence of all their customers getting attacked, and make sure that the defense is passed on to all the customers. This is simply not possible if you are running an on-premises data center. Everything you want, like a firewall, or a gateway, or any of that can be built in cloud with native services. And network policies which are simply XML/JSON text can be tweaked from existing samples, which is far superior to anything that existed before."*

IC 5: Physical and Environmental Safety

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Security of the Cloud is the responsibility of the Cloud Provider.

NCIIPC conducts audits on notified systems to evaluate their adherence to the guidelines. The shared responsibility model of the cloud implies that its physical security is the cloud service provider's responsibility. Cloud service providers do provide the steps that they take to ensure physical and environmental safety of their data centers (AWS[37], Azure[38]). Additionally, third party audit certificates are available to demonstrate compliance with global standards and processes. In India, CSPs need to be empaneled and undergo STQC (Standardisation Testing and Quality Certification) audit[39] before they are empaneled to offer cloud services to central government departments and agencies.

IC 6: Testing and Evaluation of Hardware and Software

[34] [34] AWS System Manager incurs no additional costs and can be used to access private VMs, while Azure Bastion service incurs an hourly charge.

[35] [35] Terminology used by various Cloud Service Providers are different. For instance, Azure uses the term, Application and Network security group, for security groups and Network ACLs respectively, but they perform a similar role, nevertheless.

[36] Incurs additional costs.

[37] (Amazon Web Services, n.d.)

[38] (Microsoft Corporation, 2023)

[39] (MEITY, n.d.)

Cloud providers are moving down the stack and not only own the Data-Centre OS, but also the Chips. The approach suggested by the regulator (CC-EAL) is ideal for entities that procure their own IT hardware and is not relevant for the Cloud era when hardware is a concern for CSPs and not for the user entities. Given that CSPs have also evolved their offerings to support On-premises hardware[40] via a hybrid approach and prefer to standardise the hardware to provide the best possible security controls, the guidelines must evolve to reflect this aspect.

While user entities can use native services readily available for patch management of OS, the hard problems of managing Software Bill of Materials (SBOMs), remain as discussed in IC (Implementation Control) 1: Asset and Inventory Control.

OC 1: Data storage: Hashing and Encryption

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Yes
Cost	Encryption may result in slightly higher storage costs. Key storage beyond a certain limit may also result in additional costs.

Cloud approaches encryption differently than a desktop OS centric approach, through a set of baseline services, as described below:

Identity Authentication – Supports storing secrets (passwords, 2FA Seed, Software and Hardware token authenticators) for Identity authentication. While it is possible to specify authentication methods used and relevant parameters, it is not possible to specify fine grained controls such as Cryptographic algorithm, key sizes etc., as they are managed internally by the providers.

Cryptographic Key Storage – Cryptographic keys that comply to various standards (FIPS, PCI-DSS) can be stored in dedicated key storage services, which support a range of operations such as Creation, Revocation, Signing, Rotation, Verification, Encryption, Decryption and Deletion. All operations are access controlled through the trifecta of IAM roles, policies, and identities. Providers also allow users to bring their own cryptographic keys (BYOK)[41] and connect their key stores via service proxies[42].

Secret Managers – Apart from cryptographic keys, other types of secrets such as API Keys, TLS Certificates, Database credentials etc. could be managed by native services (AWS Secrets Manager, Azure vault) or third-party services (Hash Corp Vault) hosted within the cloud, which support encryption, decryption, rotation, versioning, among others.

Service Integration – Key Vaults and Secret vaults are accessible natively within numerous services to

[40] Azure Stack, AWS Outposts and Google Anthos are examples where the hardware could be in the premises of the CII Operator, even though it is fully integrated with the Control plane of the CSPs. The On-premises hardware is treated as another region by the CSPs in their control plane APIs, with security guarantees like their own hardware, including delivery of patches, upgrades, and full stack maintenance.

[41] For a detailed discussion on Bring Your Own Keys across various Cloud Providers, the following references can be referred to:

1. Azure (https://learn.microsoft.com/en-us/azure/information-protection/byok-price-restrictions)
2. AWS (https://aws.amazon.com/blogs/security/how-to-byok-bring-your-own-key-to-aws-kms-for-less-than-15-00-a-year-using-aws-cloudhsm/)
3. GCP (https://cloud.google.com/anthos/clusters/docs/multi-cloud/azure/how-to/bring-your-own-key)

[42] Service Proxies could be any third-party Key management services. Hashicorp Vault is one such widely used proxy service.

provide encryption/decryption on the fly without user intervention, if configured by the users (e.g., VM Disks, Object Storage, DB backups, SSH keys, Emails, OS Images, Code signing etc.). As they are fully integrated with IAM trifecta for access control, implementing any type of data security control that requires encryption is possible via configuration.

Practitioners also point out that on hashing and encryption *"it is the same, as that of an on-premises environment. It is the same operating system, it has the same applications, the same network. The only difference is that the network ensures that the server is not in the same building as them. All encryption controls including the commercial compliances out there, PCI included, happily accept cloud controls and the governance around them."*

OC 2: Incident Management

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Yes
Cost	Depends upon the solution.

The guidelines do not define what an incident is and leave that to the CII entity. CERT-In directions however identify a list of 20 cyber incidents. Cloud service providers, however, have various native and third-party tools that allow managing incident reporting and automated responses.

For instance, AWS has a native Incident manager, which when combined with log analysis, event ingestion and system manager tools, allows automated response plans using runbooks and Lambda routines. It is also possible to use only some tools and create incidents in any external tools, using APIs, via Lambda routines. Similar functionality is available in Azure Sentinel with slightly different characteristics (Cloud Functions, Run book automation via Power shell etc.).

The advantage of native tools is that they tend to play with IAM trifecta of Identity, Roles, and policies very well, while third party tools may require additional setup and configuration.

Practitioners point out that *"The only thing not available for the Security Operations Center (SOC), when you have moved to the cloud is the physical access to the server, and the cables. Now they must just monitor the network usage between the NOC and wherever the public cloud region that they are hosted in. Right beyond that, there is no difference at all. So, they can get the same type of incident management process, the same software, the same stack, the same people who are trained in that continue to do so do the same thing. Even SIEM (Security Information and Event Management), packet flow analysis, subnet and host monitoring are more efficient in the cloud. So, you could do some things less and still get better security."*

OC 4: Data Loss Prevention

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Yes
Cost	Depends upon the solution.

For an effective Data Loss Prevention implementation, the following capabilities are essential:

Data Asset Enumeration – Data asset discovery is a solved problem in cloud because all resources can be enumerated via APIs. The APIs, however, cannot detect sensitive data stored deep within block storage devices, under a file system / volume manager, which requires explicit discovery through agents installed within Virtual machines. Incremental discovery is also easy, as resource creation APIs can be configured to trigger Cloud functions upon successful creation of a new asset (e.g., Creation of object store, new database in a

DB cluster, new folder in a shared file system, new object in an object store, and insertion of a new record in a SQL DB).

Data Asset Classification – Classification is typically done by tags, where based on the internal requirements of the entity, a data asset is marked as Sensitive, Confidential, PII. Any given data asset can have multiple tags, which allows the application of any type of DLP (Data Loss Prevention) policies. Providers also have native (Azure Purview, AWS Macie) and third-party tools (Symantec) that have both rule-based classifiers and AI/ML classifiers that work at a sectoral level.

Access Policies – When combined with IAM trifecta, access policies, based on tags, can be highly effective in limiting data loss by restricting access to certain identities and roles. Policies can also be used for selective encryption of structured fields (in a DB), or entire documents (Object store) based on classification, using Key managers.

Access Monitoring for Anomalies – When coupled with other techniques described in perimeter protection, incident monitoring and network traffic analysis sections above, anomalous access can be detected and quarantined.

Practitioners note that *"Cloud has a metadata service, which allows you to tag things. With the right access, it is possible to look inside object stores, block stores, and any running servers, to create hot backups, without losing any data and run your scanning and audit on the backup snapshot. All that is available. The data loss prevention process can be completely replicated or can be improved. If in the cloud, you can tag data while it is flowing from one place to the other at the time of generation or storage, right rather than doing it after the fact. But it is, again, a unique way to do it. But it is doable."*

OC9: Critical Information Disposal and Transfer

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Yes
Cost	None.

The API driven approach used by CSPs for resource management makes it trivial to delete data by deleting resources. When combined with other techniques like Encryption and Bring Your Own Keys, it makes it impossible for even CSPs to have access to data stored in Physical storage devices before they are fully zeroed out. Transfers to other accounts can be carried out through the well-established trifecta of IAM, Policies and tags.

DR (Disaster Recovery) 1,2,3: Disaster Recovery and Business Continuity Controls

Parameter	Summary
Relevance in Cloud	High
Supported in Cloud	Yes
Cost	Depends upon the solution.

Business Continuity – There are several techniques available to ensure that services/applications hosted in the cloud do not go down. Providers support multiple availability zones within a geographical location, and several geographical locations within a continent/nation state boundary, with Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). Further they also provide auto scaling groups and native support for clusters (mostly based on Kubernetes). Both Native and third-party DB services (e.g., Snowflake) also provide automatic failover in the case of disruption in an availability zone.

Data Backups – Several options exist for data backups across geographies and availability zones for various databases and object stores. Object stores can be replicated across accounts and are excellent candidates to hold incremental backups. Using different accounts and geographies and availability zones for backups allows implementing the Hot, Warm, Cold disaster site design as recommended by the guidelines.

Conclusion

As the analysis indicates, it is possible to implement all the analysed controls in the cloud environment. However, several controls, being very generic in nature, need to evolve and be refined further, if they must be relevant.

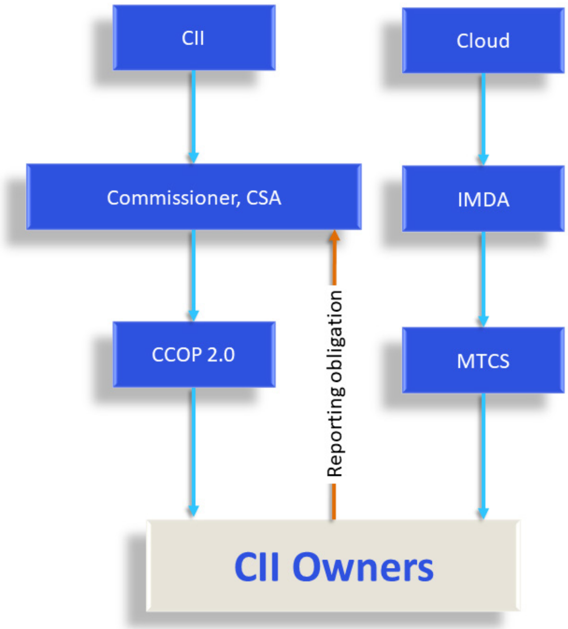
4 Regulatory Analysis of Other Countries

SINGAPORE

Relevant Legislation and Agencies

In Singapore, the Cybersecurity Act[43] is the broad legislation that establishes the legal framework for national cybersecurity. The key objectives are four-fold:

- Protection of CII.
- Authorise the Cybersecurity Agency of Singapore (CSA) to prevent and respond to cybersecurity threats and incidents.
- To establish a framework for sharing cybersecurity information.
- To establish a licensing framework for cybersecurity service providers.



The Cybersecurity Code of Practice for Critical Information Infrastructure (CCOP 2.0)[44] is the second legislation that governs CII. It specifies the minimum cybersecurity requirements to be implemented by CII owners and operators.

The Cyber Security Agency (CSA) of Singapore oversees cybersecurity practices and compliance with laws. The Commissioner of CSA, appointed under the Cybersecurity Act, is responsible for the designation and withdrawal of CII status, issuing codes and written notices, and conducting cybersecurity exercises for CII owners.

CII Owners are mandated to report cybersecurity incidents to the Commissioner. They are also required to conduct an annual cybersecurity risk assessment, and audits of the compliance of CII with the Act and CCOP at least once every two years by an auditor approved or appointed by the Commissioner. Non-compliance with the law leads to the imposition of penalty in way of fines or imprisonment. An appeals process, which is provided under the Cybersecurity Act, enables aggrieved CII operators and owners to appeal against a decision made by the Commissioner[45].

Standard Setting and Cloud Adoption Approach

The standards for cloud adoption, and other industry-specific standards, are established by the Singapore Standards Council in collaboration with industry, government, and academic organisations. The INFOCOMM and Media Development Authority (IMDA) manages the standardisation work of the IT Standards Committee within the Council[46].

The IT Standards Committee oversaw the creation of the Multi-Tiered Cloud Security (MTCS) Standard to encourage secure cloud adoption practices across industry. Popularly referred to as MTCS SS 584, it is based on the ISO 27001/02 Information Security Management (ISM). IMDA oversees the adoption of MTCS and encourages the same in two ways - primarily, by way of third-party

[43] (Republic Of Singapore, 2018)
[44] (Cyber Security Agency of Singapore, 2022)
[45] Republic of Singapore, 2018, Article 14
[46] (Republic of Singapore, n.d.)

certification scheme, and then by self-disclosure of service- related information by CSPs.

While the MTCS certification is voluntary, an SS584 certification is mandatory for CSPs wanting to acquire bulk government tenders[47]. Since, adoption of cloud would qualify as a change in the operation of the CII, the Cybersecurity Act applies to both government and private CII owners, who are obligated to follow the rules on notification, audit, risk-assessments, cyber-security exercises, and reporting of incidents.

Failure to adhere to these requirements could result in a fine or imprisonment. The MTCS is a tiered standard that certifies a CSP's security services as Tier 1, Tier 2 or Tier 3 based on their ability to secure low, moderate, or high impact data, respectively. A CII entity will choose a CSP that is certified at Tier 3, the highest level of certification that validates the ability of a provider to deal with high-impact data that is critical.

Notably, the tiered approach to certification acknowledges the varying degrees of security needs in the demand for cloud. While the MTCS certification requires the involvement of one of the five IMDA-identified Certifying Bodies, self-assessment and third-party auditing are widely accepted. CSPs and CSP customers are also encouraged to routinely self-furnish audit reports, and other information related to their cybersecurity posture, indicating that consumer awareness is central to Singapore's cloud adoption strategy.

Doctrine

The approach to certification of CSPs for cloud-security is risk-based and light touch. It is light touch since certification is voluntary, but compliance is mandated only around matters of cybersecurity and incident reporting. Auditing requirements are also not intensive and light touch regulation, and harmonisation of standards can be identified at the core of its cloud doctrine.

Key Takeaways

Singapore's regulatory approach towards cloud and CII has been underscored with the recognition that regulation of cybersecurity needs to be balanced with the larger economic aspirations of the country. This is demonstrated by:

- Proactive harmonisation of the MTCS with other international standards and frameworks. The ability for a CSP to get cross-certified leads to fewer compliance difficulties, and more diverse cloud offerings being made available to citizens and businesses.

- The involvement of industries and stakeholders in both standard setting and regulation. The MTCS was industry-led and CCOP 2.0 was framed based on public consultation by actively involving domain experts and academics in the regulatory processes, the government ensures transparency in its cybersecurity decision-making. This ensures quality while fostering public trust.

- The provision of an appeals process further ensures transparency since the Commissioner's decision can be reviewed by an independent advisory Panel, while giving CII operators a platform to represent their interests.

JAPAN

Relevant Legislation and Agencies

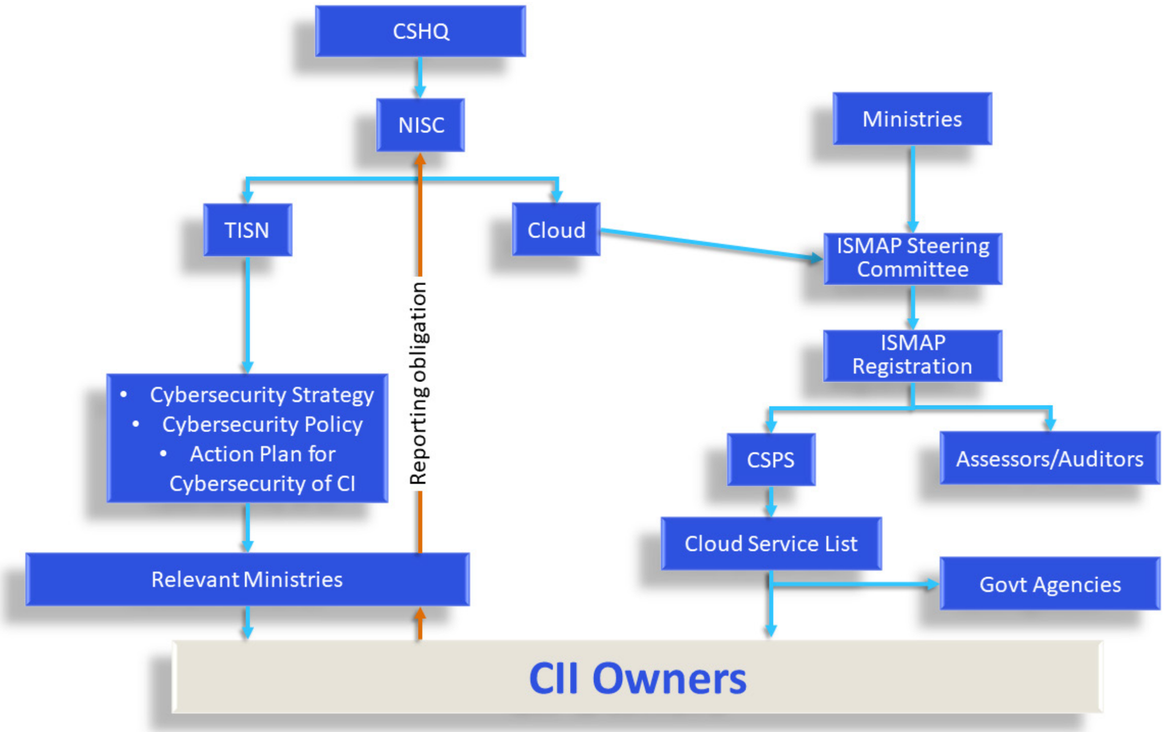
In Japan, the Basic Act on Cybersecurity[48] (BAC) is the parent legislation establishing a framework for critical information infrastructure[49],. and

[47] ibid

[48] (The Government of Japan, 2020)

[49] The Government of Japan, 2014, Article 3.1

sets out the basic principles and measures for cybersecurity[50]. The BAC applies limited obligations on CII operators and expects them to voluntarily, but proactively, pursue best cybersecurity practices established by various industry-specific guidelines.



Article 12 of the BAC mandates the creation of a Cybersecurity Strategy, which was created in 2015 and amended in 2021[51]. The regulatory bodies relevant to CII are the Cybersecurity Strategic Headquarters (CSHQ), which was established by mandate of the BAC, and the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) which takes on the role of the governmental CERT. The NISC acts jointly with the CSHQ to promote cybersecurity policies for CII.

The NISC formulated the CSHQ's Cybersecurity Policy for Critical Infrastructure Protection, 2022 (Cybersecurity Policy) to operationalise the Cybersecurity Strategy and provide specific Guidance to CII sectors. It identifies the fourteen critical information sectors under the CSHQ and five ministries responsible for critical infrastructure protection. The Cabinet Secretariat and responsible ministries collect information on the execution of the Cybersecurity Policy and provide feedback that informs the formulation of guidelines and principles.

In 2022, the NISC also released the Action Plan for Cybersecurity of Critical Infrastructure, which includes its fourth Action Plan for Information Security Measures for Critical Infrastructure. The action plan details requirements for CII operators to strengthen response systems, risk management processes, and safety standards. Other than the Cybersecurity Policy and the Action Plan, government entities are further subject to the NISC's Common Standards on Cybersecurity Measures of Governmental Entities. CII operators, both private and government, can be subject to

[50] (Onodera, Tanaka, Tsuta, & Shimamura, 2023)

[51] (The Government of Japan, 2021)

guidelines issued by responsible ministries as well as reporting obligations under Japan's personal data protection legislation (APPI).

Cloud Certification (ISMAP)

The NISC is also involved in the development and operation of the Information System Security Management and Assessment Program (ISMAP), along with the Digital Agency, the Ministry of Internal Affairs and Communication (MIC), and the Ministry of Economy, Trade, and Industry (METI). ISMAP is a risk-based compliance-centric registration system for CSPs and establishes a basic framework and process for their assessment.

The apex body governing ISMAP is the ISMAP Steering Committee, which is established by the ministries. The Steering Committee establishes the requirements for CSPs and auditing entities, and standards for information security management and operation. ISMAP is based on USA's FedRAMP model. It endorses auditors to report on the cybersecurity posture of CSPs wishing to be ISMAP certified[525] Once approved, CSPs are published on the ISMAP Cloud Service List. Government agencies may only procure services of CSPs listed by the ISMAP Steering Committee. The certification remains valid for 16 months.

The ISMAP Steering Committee exercises the right to investigate certified CSPs and auditors to monitor compliance status, and based on their findings, demand re-assessment or re-application. However, compliance with the System is also enforced by a formal pledge that CSPs take at the time of registration. The pledge requires them to provide the procuring ministry with any additional information they may require, report security incidents without delay, cooperate in monitoring processes, and comply with the regulations outlined with the Rules, Basic Regulation, and other documents and laws that the Japanese government might issue. CSPs are also required to notify the ISMAP of significant control changes. Failure to comply results in a revocation of the CSPs certification.

CII operators remain primarily liable for making an informed selection of its CSP based on their cybersecurity posture and the operator's security needs, while CSPs remain responsible for their own security controls, CII operators are not legally bound to report cybersecurity incidents. However, the CSHQ encourages CII operators to voluntarily report incidents to NISC via their responsible ministry[53]. Since reporting is not mandatory, the Cybersecurity Policy establishes information sharing networks through CEPTOAR (Capability for Engineering of Protection, Technical Operation, Analysis and Response) organisations[54]. The CEPTOAR Secretariat collaborates with responsible ministries for collecting incident information from CI operators and collaborates with the Cabinet Secretariat in times of cybersecurity crisis.

Doctrine

The cloud framework of Japan is more compliance-oriented than its counterparts in other jurisdictions. Under the ISMAP Steering Committee, specific guidelines on controls are furnished[55]. While incident reporting is not mandatory, the Steering Committee remains regularly updated on the operational configuration of cloud arrangements used not just by CII operators, but all entities using CSPs. Since the Committee possesses the ability to issue audits and investigate compliance status, the regulatory burden on CSPs is higher due to the recurring need to demonstrate compliance. Japan follows a standardised approach to cybersecurity

[52] (ISMAP Registration Committee, 2022)

[53] (Onodera, Tanaka, Tsuta, & Shimamura, 2023)

[54] (The Government of Japan, 2021)

[55] (ISMAC Steering Commitee , 2022)

through procuring mechanism centered around certification.

Key Takeaways

Japan's framework relies heavily on its information sharing mechanism. CEPTOAR allows for crucial information to be exchanged between ministries. This can be a valuable tool for crisis management since CEPTOAR networks can collect intelligence from liaisons of responsible ministries and help the Cabinet Secretariat and the NISC improve its incident response capabilities.

Australia

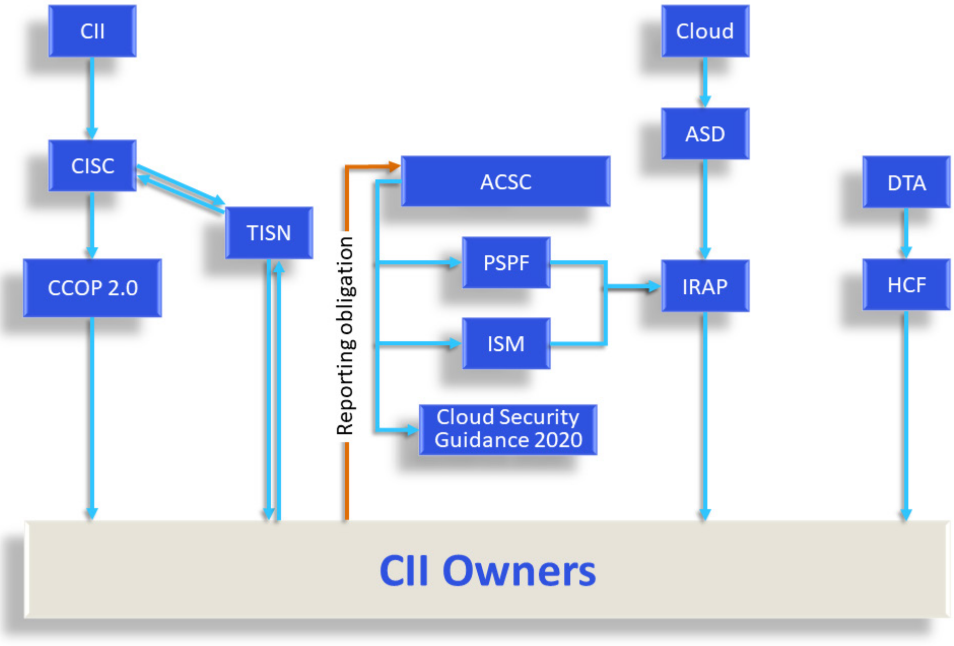
Relevant Legislation and Agencies

CII is regulated by the Security of Critical Information Infrastructure (SOCI) Act, 2018[56], which empowers the Ministry to prescribe an asset as CII. Currently, eleven sectors are identified as critical infrastructure.

Australia has also passed the Security Legislation Amendment (Critical Infrastructure Protection) (SLACIP) Act 2022, which builds on the SOCI Act to impose new government assistance obligations and cybersecurity notification obligations. The amendment requires:

1. CII owners and operators to establish, maintain, and comply with a risk management programme.
2. Establishes a framework of enhanced security obligations for Systems of National Significance (SONS), a subset of CII assets that are of national significance.
3. Expands reporting and government assistance obligations.

Support and guidance for CII operators is provided by the Australian Cyber Security Centre (ACSC) which is a part of the Australian Signals Directorate (ASD), and the Cyber and Infrastructure Security Centre (CISC) which operates under the Department of Home Affairs. The CISC is tasked with monitoring compliance with the Register of Critical Information



[56] (The Australian Government, 2022)

Infrastructure, which is a database of information about critical infrastructure assets maintained by the Secretary of Home Affairs. The Register enables the government to track ownership and operational arrangements for CII and understand any interdependencies to inform their view of the threat environment.

The CISC encourages compliance with initial and ongoing obligations of responsible entities to provide information to the ACSC, even if the threshold for mandatory reporting is not met[57]. Failure to comply with reporting requirements results in a civil penalty. In addition to limited mandatory reporting requirements, the Australian government leverages the Trusted Information Sharing Network (TISN) as a primary engagement mechanism with CII entities[58]. The TISN allows CII entities to better understand and mitigate risk with a sector-specific understanding of cybersecurity threats and risks.

Regulation of Cloud (IRAP)

While there is no longer a certification requirement for CSPs, the ASD administers the Infosec Registered Assessor Program (IRAP), a compliance program that provides government and industry with security assessment services through qualified and experienced cybersecurity professionals. The adoption of cloud is overseen by three agencies, namely, the ASD, the ACSC, and the Digital Transformation Agency (DTA) which oversees the government's digital transformation progress.

Mandatory guidance and obligations for agencies looking to adopt cloud are outlined by the Protective Security Policy Framework (PSPF) and the ACSC's Information Security Manual (ISM). These function as codified advice from the ADS and ACSC, and are supported by various other guidance, such as the Secure Cloud Strategy, and similar plans issued by the government.

IRAP is mandatory for all Australian federal, state, and local governments that avail cloud services. Therefore, a commonwealth entity that owns or operates a critical asset must avail itself of an IRAP-empaneled CSP. The IRAP programme demonstrates that trained professional auditors remain crucial to Australia's certification approach, and therefore to ensuring cybersecurity. IRAP assessors provide third-party assessments to examine an entity's cybersecurity compliance to practices established by the ISM and PSPF, identify security risks, and suggest mitigation measures. Following the assessment, assessors provide an IRAP-endorsed report to CSPs that can be shared with potential cloud-customers so that they may make an informed CSP selection most suitable to their data's security needs . To maintain the accuracy and currency of the assessment report, CSPs are permitted and encouraged to conduct self-assessments and detail changes made to their security and services, for which they may or may not avail themselves of the services of an IRAP assessor.

The Cloud Security Guidance, 2020 provides CSPs, cloud customers and IRAP assessors with resources to ensure that continued risk-based assessments can be facilitated. The DTA's Hosting Certification Framework, 2021 requires vendors wanting to obtain government contracts to certify themselves as either Strategic or Assured. This certification forces CSPs to more stringent reporting, review, and change disclosure obligations.

CSPs are encouraged to re-assess their security and cloud services every 24 months, or upon the occurrence of certain events that necessitate a revalidation of their security posture. CSP accountability is managed through contracts, with the procuring agency being responsible for their own risk management activities and ensuring

[57] (The Australian Government, 2022)

[58] (The Australian Government, 2023)

that all residual risks have been subsumed by appropriate authorities.

Doctrine

CSPs, cloud users, and IRAP assessors are provided with multiple guidance documents and information to ensure compliance with best practices as well as existing laws. The framework followed is principle-based, with risk-mitigation being the primary objective. There is little compliance burden with audit requirements and few possibilities of a mandatory reporting obligation. A cloud-user who is a commonwealth entity, and/or, a responsible entity for critical assets, will face a higher degree of compliance with audit requirements and mandatory reporting obligations.

Australia also emphasises that informed users and trained auditors play a key role in cloud adoption. Transparency and awareness of a provider's cybersecurity controls, and posture is seen as crucial to an agency's ability to service its own security needs. This enhances accountability while avoiding a 'one-size fits all' approach.

Key Takeaways

Australia's approach demonstrates the following advantages:

- By instituting TISN, Australia furthers the engagement between government and industry by continuing to take inputs after a regulation has been introduced. Unlike Japan, it does not restrict cybersecurity-intelligence sharing to ministries alone. Rather, TISN acts as an ongoing communication mechanism that keeps both the government and the CII operators updated on security risks.
- Efforts to enhance auditing capabilities can have valuable payoffs. The training of auditors under IRAP prevents skill and knowledge redundancy and ensures better quality risk assessments.

GERMANY

Regulation of CII

In Germany, Critical Information Infrastructure, or KRITIS[59], is regulated by the Federal Office for Information Security (BSI) under Germany's IT Act. Ten sectors are identified as critical sectors under Section 2(10) of the BSI Act. The BSI KRITIS Regulation identifies systems as critical within the meaning of the BSI Act and specifies "threshold values" for categories of asset infrastructure. When an asset reaches or exceeds the threshold value for its asset category, it counts as critical infrastructure. The Federal Office of Civil Protection and Disaster Assistance (BBK) also participates in the protection of CII.

Obligations for CII operators are specified by the German IT Act and BSI's KRITIS regulations. Operators with a level of supply exceeding a threshold value are obliged to establish contact and reporting channels with the BSI for the submission of reports[60]. Reporting obligations do not apply to critical infrastructures below the threshold values, though they may still voluntarily report incidents. The energy sector is an exception since all entities in the sector are subject to statutory reporting after the implementation of the European Network and Information Security Directive (NIS Directive). Failure to comply with the BSI requirements can result in a fine of up to twenty million euros.

Notably, the draft version of the European Union Agency for Cybersecurity (ENISA)'s European Union Cybersecurity Certification Scheme for Cloud Services (EUCS) draws significantly from C5's security standard[61]. Furthermore, Germany has also adopted a unique approach to ensuring

[59] (Federal Office For Information Security, n.d.)

[60] ibid

[61] (Federal Office for Information Security)

CII cybersecurity through the UP KRITIS initiative which is premised on the principle of joint action by state, society, and businesses. It is a private-public cooperation initiative between KRITIS operators, their associations, and the relevant government agencies.

Regulation of Cloud (C5)

Germany regulates cloud through an auditing standard known as C5, or Cloud Computing Compliance Controls Catalogue. The C5, which was published by the BSI in 2016, establishes mandatory minimum and advanced security baselines to be followed by government agencies and organisations that work with government agencies while procuring cloud solutions. It is also increasingly being adopted by the private sector. Cloud customers can determine for themselves whether the baselines established by the C5 are sufficient for their operations and may specify additional requirements to be met by their CSP. C5 is based on internationally recognised IT security standards like ISO/IEC 27001:2013, the Cloud Security Alliance Cloud Controls Matrix 3.0.1, and BSI's IT-Grundschutz Catalogues.

The auditing system is shaped to ensure transparency to users and convenience to CSPs. The C5 addresses 114 controls over seventeen domains, and guides CSPs on a range of issues such as organising informational and physical security, processing highly confidential data, and ensuring high availability and security. It also establishes surrounding parameters that require a corresponding audit report that contains a comprehensive description of the IT system as well as information on matters like jurisdiction of data storage and processing, the disclosure obligations, and investigatory powers of these jurisdictions, and the CSP's existing certifications and attestations.

Auditing is carried out by Certified Public Accountants, ensuring that the C5 audit is as rigorous as an annual financial audit. Audits cover a period of twelve months, but not less than six months, and are supplemented with "attestations" made by CSPs which acts as a statement on the ongoing appropriateness and effectiveness of the CSP's safeguards. This allows cloud customers to make an informed decision about a CSP's ability to meet their security needs. Furthermore, the auditing system instituted by C5 reduces redundant auditing. Reporting obligations of CSP's in the event of cyber incidents is mandated under Section 8c (3) of the BSI Act and applies to security incidents that have a significant impact on the provision of digital services.

Cloud Doctrine

The C5 adopts a controls-based approach by summarising targets and objectives that a CSP must fulfil and making a distinction between mandatory and optional requirements. While other cloud frameworks discussed are premised on mitigating risk, the C5 is notably premised on ensuring transparency. It also aims to develop a reasonable framework and strategy through conversations with cloud providers and users. The involvement of industry has also ensured that the framework is scalable. The use of international frameworks and standards in developing the C5 has also ensured that it remain interoperable with other security standards. Furthermore, it remains committed to revision and being updated in accordance with technological developments. The newest version of C5 is C5:2020 which was released in 2020 after being revised in 2019, and increases the scope of C5 by adding new requirements.

Key Takeaways

- The C5 is frequently updated through a process that receives inputs from CSP providers and users. This reduces redundancy in audits, barriers to business operations and scaling efforts, while also ensuring choice to consumers.
- International standards are used as the basis for certification. This reduces the overall effort required, since it combines multiple compliance audits. This allows the principle of

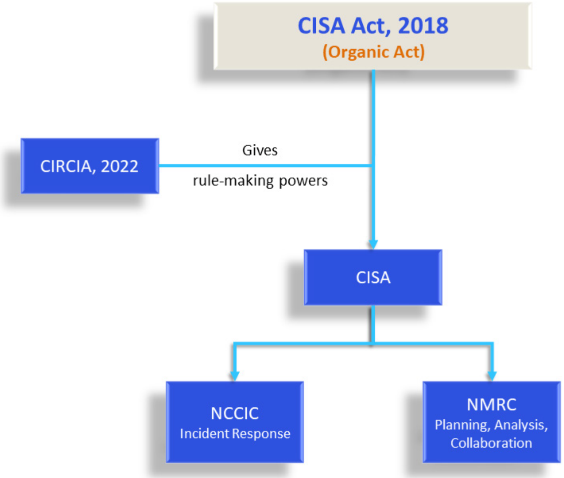
transparency to be operationalised effectively.

- UP KRITIS is a unique private-public partnership system that operationalises collaboration to effectively implement KRITIS related initiative and programmes. It also works to foster mutual trust.

United states of America

Relevant Legislation and Agencies

The 1998 Presidential Policy Directive titled, "Critical Infrastructure Protection"[62] called for national unity of effort for achieving its objective. This set the tone for US's CI Policy, which focusses on co-ordination among sector-specific agencies and federal departments, and strong collaboration with CI owners and operators.



The Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018 rebranded Department of Homeland Security's National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency of USA.[63] CISA is the main organisation for federal cybersecurity and works as the national coordinator for security and resilience of critical infrastructure.

CISA helps CII entities in better managing their cybersecurity risks by enabling the use of National Institute of Standards and Technology's (NIST) Cybersecurity Framework in conjunction with sectoral regulations of critical sectors. Information sharing and cooperative action across the private and public sectors have been recognised by CISA to be the touchstones of improving the nation's collective defence.

Recently, CISA collaborated with United States Digital Service and FedRAMP to develop the Cloud Security Technical Reference Architecture (TRA) to function as a guidance for agencies – government or private, while migrating to cloud.

Regulatory approach

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was signed into law in March 2022. The Act gives rule-making power on cyber incident reporting to CISA and will now transform it from a partner organisation to a regulatory enforcer with the legitimate power to enforce compliance.[64] Notably, CISA is mandatorily required to consult with various entities throughout the rulemaking process.[65] Furthermore, CIRCIA also provides substantial protections to entities who report either mandatorily or voluntarily to CISA. This rule-making process is currently underway.

Cybersecurity frameworks for CI owners and operators are developed by the National Institute of Standards and Technology (NIST). The NIST is an agency under the U.S Department of Commerce since the 1988 NIST Act. Its mandate to create such frameworks is granted by the Cybersecurity Enhancement Act of 2014. In February 2014, NIST published its **Framework for Improving Critical Infrastructure Cybersecurity,** which is available

[62] (The White House, 1998)

[63] (Brumsfield, 2019)

[64] (Doubleday, 2022)

[65] (CISA, 2022)

for use by all organisations, but is mandatory for U.S. Federal agencies.

The CSF 1.1 of 2018, currently in use, stands out because of its consultative approach, and continual updates based on a constant feedback loop, which have contributed to the document being inclusive, pragmatic, and futuristic. It is a highly informative and useful practical guide for CII entities looking to adopt cloud.

NIST also sets standards and guidelines for categorising information and information systems. Its Federal Information Processing Standards Publication (FIPS PUB 199) categorises potential impact of security breach on an organisation into three categories: *low, moderate,* and *high.* The US government's **Federal Risk and Authorisation Management Program (FedRAMP),** which works to promote secure cloud adoption across the federal government, is built upon the FIPS PUB 199's categorisation of security baselines.

The FedRAMP Marketplace Version 2.0[66] is the online repository where federal agencies may choose from FedRAMP authorised Cloud Service Offerings (CSOs). CSOs are listed on the Marketplace as *FedRAMP Ready, FedRAMP in Process,* or *FedRAMP Authorised* based on the authorisation stage they are in. Earlier, CSOs had to get re-assessed every 3 years, but now that is only necessary if the Agency Authorising Officials require it.

The federal government's selection of a CSO is based on the CSOs assessment by a third-party organisation (3PAO). FedRAMP, therefore, requires 3PAOs to be accredited to ensure that they meet their independence, quality, and knowledge requirements. 3PAOs are required to comply with FedRAMP requirements and follow their ISO/IEC 17020 QMS. NIST and FedRAMP have collaborated to develop a conformity assessment programme to produce consistent, independent third-party assessments of security controls of CSPs.

Doctrine

The USA has adopted a risks-based approach to cybersecurity. It has robust cybersecurity frameworks and effective PPPs, making it inclusive and pragmatic. Its focus on standardisation of frameworks, third party audits, harmonisation of sectoral regulations, and extensive guidance, colours it favourable for using cloud in CII.

Key Takeaways

- CISA's collaborative organisational charter has contributed towards consolidation of all federal and sectoral security requirements for CIIs in one place, and formulation of harmonious principle-based guidelines.
  ○ The NIST frameworks are robust and developed in collaboration with stakeholders. They align with international best practices, which enables ease of doing business for Cloud Service Providers (CSPs) across the globe. They do not aim to achieve a one-size-fits-all approach for all critical infrastructures and leave customisation of cybersecurity risks management to the organisations.
  ○ FedRAMP process is well defined, with abundant guidance for onboarding of a CSO. The third-party certification requirement for CSO and robust FedRAMP approval process lends confidence to federal agencies to move their critical functions to cloud.

CONCLUSION

The growing adoption of cloud across CII has necessitated the need for its regulation. The way this has been done differs from jurisdiction to jurisdiction, and yet some common themes emerge in the cloud policies discussed above.

First and foremost is the recognition of the utility of cloud and the function of governments in

[66] (The United States Government, 2021)

enabling its secure adoption in critical sectors. Towards this end, cybersecurity policies specific to cloud have proved useful in lending certainty about the regulatory environment. Second, security on cloud is a shared responsibility between a CSP and the cloud user, and therefore, guidance on how to achieve it is abundantly circulated in the jurisdictions discussed above. Third, most jurisdictions are adopting a principle or risk-based approach to cloud security. Fourth, a standardised process for cloud certification for CII helps achieve compliance across sectors. Furthermore, alignment with international standards helps in cross-certification and fosters ease of doing business. Fifth, a robust auditing process, comprised of independent third-party audits, helps maintain a robust cloud security posture and ensures security of CII.

Most of the model laws on cloud security in CII are a result of consultation, coordination, and collaboration. Laws that are drafted in consultation with stakeholders, such as CSPs, industries, academic institutions, etc. are found to be more robust and easily implementable. Coordination between the central CII authority, incident response authority and sectoral regulators is key to maintaining the cybersecurity posture of CIIs and reducing redundancies. Collaboration between the government, CII entities and CSPs maintains transparency, creates trust, and helps build capacity which is otherwise hard to achieve in siloes.

5 Insights from Interviews

Methodology

- Representatives from key sectors of finance, transport and infra, and power and energy were approached.
- All the participants were provided a questionnaire[67] before the interview.
- Participants were given an option of choosing to reveal their names, title, and the organisation they are associated with. In the case they were not willing to come on record, only their position is noted (e.g., Regulator, Auditor, SOC Operator).
- Interviews are recorded and transcripts were then analysed, and relevant sections are summarised.

Financial sector

Advantages of Cloud

A senior RBI official remarked that *"The key performance matrix that digitisation success of the financial sector is measured against, comes down to two aspects – convenience and security. Cloud has clear advantages for the BFSI sector from every angle, such as better security, faster turnaround time, and operational resilience."*

Another senior RBI official added that *"The advantages of cloud are in terms of scalability, agility with less turnaround time, and cost effectiveness. CSPs also bring to the table an extremely elevated level of expertise in terms of manpower, services, and technology. Due to this, their solutions are better and cheaper. Shared services such as public or community cloud, are especially useful for cooperative and regional banks, who cannot afford standalone solutions. Cloud is also useful for achieving RBI's goal of financial inclusion. Shared services on cloud can bring down cost and this cost benefit can be passed down to the customers."*

A Chief IT Officer of a bank remarked that *"For BFSI entities, Cloud offers them a faster time to market, elasticity, better security services, and high availability due to solutions panning across many data centers."*

Adoption hesitancy

The interviews indicated that, despite the advantages cloud offers for the financial sector, no bank has placed its critical workload on cloud. When probed regarding the reasons for hesitancy that have hindered acceptance of cloud, the following issues emerged as the key causes from the regulators' perspective:

- Regulatory compliance – From the regulator's perspective, achieving enforceability of their functions is essential. Currently, the dual problem of multiple regulators and dominance of a few CSPs has hindered their ability to adequately enforce compliance.
- Attributing responsibility – The shared responsibility model makes the CSP and the user entity equally responsible for cybersecurity on cloud. This model makes it hard for regulators to fix responsibility on one entity in a breach. Regulators find it difficult to enforce their regulations on CSPs and this is a cause for worry for them.
- Cloud audits – There is a need for establishing audit requirements for CSPs such as security audit, performance audit, availability, and privacy audit. CSPs also need to indicate their Business Continuity Plans and Disaster Recovery services and Continuous Monitoring capabilities.
- Data privacy – BFSI entities hold financial data in a fiduciary capacity. In the absence of a robust data protection bill, the problem of data privacy looms large over India. The proposed Digital Personal Data Protection

[67] The questionnaire was specific to the sector and the role of the participant.

law is being looked at by the sector to offer some much-needed clarity on this.

- Exit strategy – It is easier to adopt a cloud environment than to exit it. This causes worry about portability and interoperability.
- Infrastructural and capacity challenges – Many organisations have legacy systems that do not support cloud. Moreover, adoption of cloud requires skilled human resources that are often lacking with organisations.

Bank CISOs pointed out the reasons for hesitancies from their side, as summarised below:

- Lack of guidance - Even though they recognize cloud as being an important and inevitable solution, businesses and organisations hesitate due to lack of regulatory certainty and clear guidelines specific to cloud adoption.
- Lack of awareness – The board of directors of each organisation is responsible for decision making regarding cloud adoption and they lack awareness about cloud and there is a tendency to distrust internal assessments about the need to move to cloud and look for a third-party validation.
- Reactive approach – Indian entities' approach to cybersecurity is often found to be reactive instead of proactive.
- Lack of expertise – Cloud is still a niche area in India and there is lack of expertise with entities to implement security measures in a cloud environment.
- Multiple regulators – Multiple regulators create further complications and apprehensions among entities, leading to a status quoist approach.

Suggested approaches to accelerate Adoption

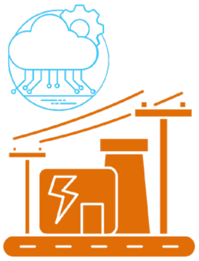
The RBI officials feel that the best approach for the RBI is to have principles-based regulations for cybersecurity in cloud, rather than a prescriptive approach, since prescriptive regulations tend to become over-prescriptive over time and cause apprehensions in the industry about their acceptance, leading them to finding ways to get around them. Any effective system must be built on a foundation of trust among stakeholders.

One of the officials suggested the formation of a Self-Regulatory Organisation (SRO) that monitors the conduct of member entities. The role of an SRO may include setting the standards for conduct as well as acting as a bridge between the sector and the regulators. This approach can help protect consumer interest and improve governance standards.

Bank CISOs however point out, that their primary need is to get cloud specific guidance from the regulator. Such guidance will inspire confidence regarding cloud adoption among board members. It will also help change organisational approach towards cybersecurity from merely reactive to more proactive. The need to manage multiple regulators being a point of concern, they point out that, there is a need for an overarching regulatory framework for cloud and within such framework, sectoral regulators can issue domain specific regulations.

All of them suggest that there is a need to create awareness regarding the utility of cloud and the requisite skilled workforce to operate on cloud, without which they would struggle on implementing the guidelines.

Power sector



An executive who was responsible for crafting the strategy for digitisation of the electricity distribution company (DISCOM) of a large northern state points out that most of the initial budget came as a loan from the central government, which then got converted into a one-time grant, upon meeting the targets. While their Cyber-security preparedness and assessment is based on CERT guidelines, they were not aware of NCI-IPC guidelines and hence were not able to comment upon its utility.

The DISCOM board has approved a proposal to use Cloud for scalability and enhanced security in addition to the current measures in place (e.g., Third Party Audits and other measures recommended by CERT), if a Cloud Service Provider is empanelled by CERT. Given that, the central government no longer provides grants, they prefer the Op-Ex model than the Cap-Ex model as it aligns their expenditure closer to revenue and hence do not see large Capex spends on IT as sustainable. They also mostly rely on system integrators to provide them the necessary support for Cyber Security controls and point out that a risk-based data classification scheme would help them in assessing which workloads would be best suited for moving to the cloud.

Infrastructure and transport sector

CIOs in this sector point out that the digitisation journey looks different for the transport sector, which is replete with legacy systems. It is the government's push for digitisation that has created some willingness to invest in digitisation. The levels of digitisation and their motivation, therefore, differs significantly from sector to sector.

Auditors who perform cyber risk assessment in this sector, point out that the NCI-IPC guidelines do not recommend a framework, and hence their auditing approach does not, however, have a universal model and it depends significantly on the client. They prefer the ISO 27001 framework over others because it is easy to understand and manage. The most pressing challenge they face is that guidelines provide a list of controls but do not indicate the means of implementing them.

Suggested approaches to accelerate Adoption

From the auditors' perspective, a uniform framework coupled with guidance on how to implement it, is most important to ease compliance. CIOs notice hesitancy in legacy organisations to move away from their organisation charts and proactively implement greater cybersecurity measures and have observed reluctance to migrate to cloud because there is neither a clear incentive for organisations, nor a strong regulatory push. Therefore, policy approaches that promote cloud by creating awareness and incentivise its adoption would be useful in catalysing cloud adoption.

Health Sector

An executive who serves as a board member in multiple health sector companies points out that, the sector's primary focus is to provide health care and enhance the experience of the patients. IT Systems' investment hence must be viewed as an ancillary item that allows patient experience to be optimal which includes not just admission, but also other aspects such as insurance claims, medication, and health records. When asked specific questions about the percentage of investment in IT systems, he remarked that it could never be more than 1 to 2% of all the expenses, as the sector itself never makes more than 18 to 20% net margin overall. Another interesting observation, he made was that, since the health sector is always a Capex heavy sector, it is not averse to investing on Capex heavy internal private cloud model, compared to the Op-ex model of public cloud model. The attraction of public cloud hence is more on agility and its capability to deliver optimal patient experience and provide a better business continuity on a full cost basis compared to internally run private cloud.

A CISO who is responsible for data security in a large private hospital remarked that given the trend of the government pushing towards a health data interchange platform, there would be a need for large Capital expenditure from the health sector, which may not be feasible for smaller players. He further pointed out that, there is an increasing trend to even store patient records in public cloud including radiological images, but not everyone has capacity to understand how to secure that, and while one may establish a whole set of protocols and processes and procedures, competency at the ground level is concerning, as recent data breaches on public health care facilities (e.g., AIIMS) indicate. He also pointed out that while it is easier to justify an investment on MRI or PET scanner, as they have well defined Return on Investment (Roi), it is harder to understand why one should invest on data security, unless there is patient preference or perception of patient experience.

Both also point out that any expenditure that is forced on the sector for compliance purposes, would necessarily result only in lower investments because of margin pressure and hence suggest industry consultation as a necessary precondition for standards definition. When asked a specific question on what would help the sector in increasing cloud adoption from a cyber-security perspective, they were unanimous that capacity building at the grass root level is the key, as without which any law or guidelines provided by the regulator would only exist on paper and not in reality.

Strategic Sector

An executive who runs a strategic enterprise, points out that "*Digitisation is driven primarily by quality and economics. Those processes that require high accuracy are targets for digitisation / automation as an error or a mistake in the same can lead to quality issues that translate to higher costs. Our digitisation plans are essentially identifying critical process that impact quality and reducing the manual involvement in the same by either upgrading or replacing equipment* ".

When asked a specific question on the percentage of budget allocated to digitisation overall, he said that it would never be more than 10% of the total expenditure. He pointed out that, in the strategic sector, the following factors hinder moving towards public cloud:

1. Lack of buy in from the senior management / board as the prevalent mindset is conservation – if you can see something and if you own it, it is under your control – if you don't then how can you guarantee its safety and retrieval.
2. Reliance on 3rd party service providers and internet dependency.
3. Perceived Lack of Control of the date (it is not on you own infrastructure).

When asked on how the sector, views public cloud across various parameters, his views are summarised in the table below:

Criteria	Importance	Fully Owned Infra	Cloud	Notes
Ease of Use	Low	⊗	✓	
Cost	Medium	⊗	✓	
Compliance	High	✓	⊗	Cost to customise for compliance will be higher if you go to cloud service provider as there is lack of internal capacity and the CSPs hence may charge a premium on consulting and bespoke solutions.
Control	High	✓	⊗	In the strategic sector the perception is that control of your data is only possible if it stays on-prem.

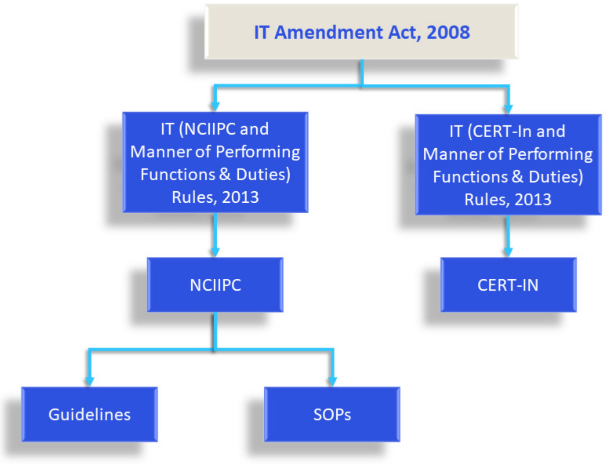
6 Regulatory Analysis of NCIIPC Guidelines

Parent legislation

The Information Technology Act, 2000 is the overarching legislation for all matters pertaining to digital infrastructure in India. In 2008, it witnessed a major amendment aimed at enhancing the cybersecurity of the country. It defined "Critical Information Infrastructure" to mean *"any computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."*[68] Subsequently, the Union Government notified NCIIPC as the national nodal agency for CII under Section 70A of the Act.

The Information Technology (NCIIPC and Manner of Performing Functions and Duties) Rules, 2013[69] give NCIIPC its charter, which includes identification of CII elements, advising on reduction of vulnerabilities, providing strategic leadership and coherence across government for responding to cybersecurity threats against CII.

Significantly, S. 4(5) of the IT Rules, 2013 makes it the basic responsibility of the organisation designated as CII to protect it. NCIIPC's role, therefore, is to co-ordinate the cybersecurity practices of CII organisations, critical sector regulators, and CERT-IN, at the national level, with the aim of securing and maintaining the cybersecurity posture of CIIs.


IT Amendment Act, 2008
IT (NCIIPC and Manner of Performing Functions & Duties) Rules, 2013
IT (CERT-In and Manner of Performing Functions & Duties) Rules, 2013
NCIIPC
CERT-IN
Guidelines
SOPs

NCIIPC assesses the criticality of the functions and services provided by an organisation and the magnitude of its impact on national security, economy, public health, and safety, in case of incapacitation or destruction of its ICT infrastructure.[70] If the functions of an organisation are found to be of *significant national impact*, then its business or industrial processes are categorised as *critical*.

At present, there are seven critical sectors designated by NCIIPC:

- Transport
- Power and Energy
- Telecom
- Government
- Banking, Financial Services and Insurance
- Strategic and Public Enterprises
- Healthcare.

Regulatory approach

The Information Technology (Information Security Practices and Procedures for Protected

[68] (Ministry of Law and Justice, 2009, Section 70)
[69] (MeitY, 2014)
[70] (NCIIPC, 2019)

System) Rules, 2018[71] further formalised the role of NCIIPC as the panoptic custodian of critical sectors, and mandated compliance with its guidelines and statements of purpose. The Rules make it within the scope of power of the NCIIPC to oversee "protected systems," which may directly or even indirectly affect CII. The interconnected and interdependent nature of cybersecurity of critical sectors necessitates that the regulator has jurisdiction over systems that have implications for national security.

The IT Rules 2018 mandate organisations having protected systems to constitute an Information Security Steering Committee (ISSC) which must also include a representative from NCIIPC. The ISSC has been made the apex body of the organisation responsible for approving all its information security policies.

The involvement of NCIIPC in the formulation of info-sec policies of the protected system may be a cause for worry for the CII entity's autonomy, especially when the regulator has a compliance centric approach. Such approach often creates a trust deficit between the government and private sector, impeding the formation of effective partnerships. Regulatory approaches in other jurisdictions such as USA let CII organisations be the arbiter of their own info-sec policies. Instead of hand-holding each CII entity, they focus on giving extensive guidance and training for creation of robust info-sec policies at the organisational level. Interviews with sectoral regulators in India also revealed that over-prescription does not cultivate trust between the regulator and the regulated entity. Regulatory frameworks based on trust promote a culture of proactive collaboration.

Compliance with the IT Rules, 2018 and NCIIPC guidelines is mandatory but little clarity exists on how to achieve such compliance. Rule-making that does not involve stakeholders may overlook the sectoral and business realities of CII and widen the gap between what is and what ought to be. While navigating the Rules, CII entities are often in want of a bridge that can help them comply with them. Countries such as the USA have made public consultations a mandatory pre-cursor to rulemaking in many cases. These consultations operate as a platform to relay the points of view of both sides which fosters trust and community building and encourages compliance instead of having to enforce it.

The lack of a clear cloud-security policy creates further apprehension about regulatory uncertainty among CII entities. Specific guidance for cloud adoption in CII are very few.

Certification of Cloud Service Offerings for the Government Sector

In 2013, the Government of India, released the GI Cloud policy, a.k.a. "Meghraj", with the vision of accelerating delivery of e-services while optimising ICT spendings of the government.[72] The GI Cloud policy came about in the context of the "Digital India Campaign", to cater to the infrastructure requirements of government departments and to reap the benefits of cloud computing.

For providing cloud services to the government, a CSP must be empaneled with MeitY.

The applicant is first assessed based on a pre-qualification criteria. This requires the CSP to be registered and be operational in India for at least 3 years, its data centre to be located in India and compliance with IT Act, MHA, CERT-In and LEA guidelines. CSPs have to mandatorily get their data centers and CSOs audited by GoI's Standardisation Testing and Quality Certification (STQC).

Once the STQC audit is successfully conducted, MeitY empanels the CSP and specifies the data center from which Cloud Service Offerings may

[71] (Government of India, 2018)

[72] (Government of India, 2013)

be provided. This empanelment is for a period of 3 years. The Government e-Marketplace (GeM) platform provides a list of empaneled CSPs, along with the bouquet of cloud services they provide and their audit status.

CSPs providing services to government entities declared as CII, have to additionally comply with the NCIIPC requirements.

NCIIPC's Guidelines for Protection of CII

The principal policy document for protection of CII is NCIIPC's Guidelines for Protection of CII[73], which apply to all CII entities. The objective of the Guideline is *"to ensure that relevant security mechanisms are built into CII as key design features."*

NCIIPC aims to continuously re-assess and update these controls in view of the dynamic nature of cyberspace and based upon experiences of CII entities. Yet, the last update was made to the Guidelines in 2015, referred to as Version 2.0.

Eight years is a long time in the cybersecurity domain and policy that is not dynamic starts losing its relevance in that period. Elsewhere in the world, best practices reflect periodic updating of cybersecurity frameworks based on a constant feedback loop from stakeholders. This helps the document to be dynamic and keep up with the developments in technology, as well as manage the emerging cybersecurity threats.

Version 2.0 lists thirty five controls grouped into five families, based upon their functional impact in the development-deployment-operationalisation cycle. Each CII is required to evaluate and take a decision about the applicability or otherwise of each control as a conscious process of minimising risk.

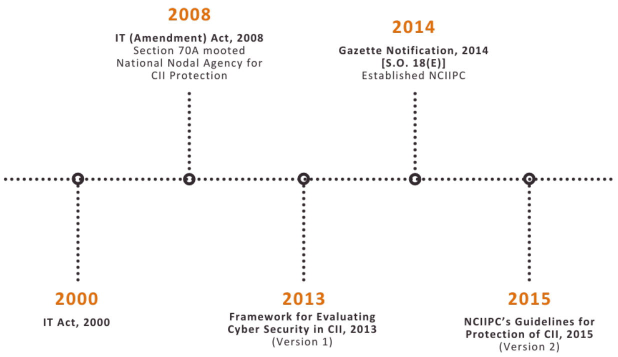
NCIIPC's controls-based prescription is different from other countries' approach to cybersecurity. In USA, a risk-based approach is taken, which allows organisations to select controls based on their effectiveness, efficiency, and constraints in view of the applicable laws, directives, policies, executive orders, regulations, or standards.[74] Singapore and Australia also follow a similar light-touch, risk-based approach. Compliance requirements for CII pertain to cybersecurity and incident reporting, with failure to comply resulting in some civil penalties in Australia. In this matter, Japan even though has a compliance centric approach , it still encourages voluntary incident reporting by CIIs without prescribing any mandatory obligations.

Interactions with stakeholders have revealed that Indian CII organisations have not yet attained cybersecurity maturity and look to the regulators for guidance on adoption of such frameworks. Achieving compliance with the controls is difficult because they struggle with understanding how to implement them. Any guideline or framework in India, therefore, needs to come with a practitioners' guide on how to implement it, with as much detail and as many use cases as possible. This would help bridge the knowledge gap among CII entities and would also cultivate confidence regarding cloud at the Board level. NIST's Cloud Security Technical Reference Architecture can be a useful reference in this regard.

From the perspective of CSPs, a principles-based approach works best. The regulators, however, use prescriptive approaches due to fears about enforceability. Sectoral regulators like RBI have pointed out that a bridge, in the form of a Self-Regulatory Organisation can be a useful model to bridge the two extremes of principle-based and control-based model.

[73] (NCIIPC, 2015)

[74] (NIST, 2018)



Conclusion

The critical sectors seek an overarching framework for cloud adoption and NCIIPC would be the right authority to develop it. This exercise, if undertaken in a collaborative spirit with the active involvement of all stakeholders, can help achieve many things for the critical sectors. It will open doors for CII entities, sectoral regulators, auditors, CSPs, cybersecurity experts and central regulators to interact with each other and work together towards a common goal. This will not only result in a robust cybersecurity framework but will also harmonise the various regulations that lie at its intersection. Once this framework is in place, sectoral regulations can become more principle-based and be harmonised with the overarching framework for cybersecurity. Uniform standards and regulations will ease compliance across sectors and therefore, promote adoption of cloud.

Singapore's experience also demonstrates that harmonising nationally developed standards with international standards and frameworks can reduce barriers to compliance and enhance ease of doing business. To facilitate cross-certification processes, IMDA frequently releases guidance and gap analyses for consumers and CSPs to help map MTCS controls with different standards. India can adopt a similar approach, which will provide much needed guidance to auditors and consumers of cloud and help CSPs diversify their offerings. A clear regulatory framework which also aligns with international standards and best practices will boost confidence of CSPs about investing in India.

7 Recommendations

NCIIPC Guidelines need to be revised

With the last update to the Guidelines made in 2015, eight years is a long time in the Cyber Security industry for a guideline to remain relevant. As the technical analysis of these guidelines indicate, it is not possible to evaluate the implementation applicability of many controls, as they are either too generic or not relevant, even by security practitioners. A comparative analysis of other jurisdictions reveal that standards are updated at a 2-to-3-year cadence, at the very least.

The guidelines must not only be revised, but should also add implementation guidance for entities, on Cloud adoption, as the entire ecosystem (CI Entities, Auditors) struggle to adapt to the guidelines in practice.

cloud security regulatory framework should be harmonised

A cross sectoral analysis of regulatory framework on cloud security shows that there are three different approaches adopted by the regulators:

- Controls based - The NCIIPC guidelines.
- Principle based – The RBI Master directions on IT Outsourcing.
- Principle based – SEBI Framework for Adoption of Cloud Services.

Furthermore, there is also deviation in the standards that entities must adopt. For instance, none of the SEBI, RBI and NCIIPC frameworks specify the standards for entities to follow, but the IT Rules, 2011 suggest it should be ISO 27001 based. This leads to severe confusion for both the entities, boards, and auditors on how to go about implementing controls and auditing them, as there is no way to harmonise practice on differing philosophies and lack of standards.

Internationally, however there is an effort towards defining standards first, and then an overarching principle-based approach, with sectoral regulators fine tuning guidelines within the larger ambit of standards and principle in consultation with Cloud Service Providers and Entities, with extensive guidance on implementing those, via risk assessment frameworks.

A shift towards this approach would reduce the compliance burden on CI entities, which might end up under different sectoral regulators and improve their cybersecurity posture.

Adopt Data classification for impact and risk assessment

While the controls-based approach forms the basis for the NCIIPC guidelines, it is at the other end of the spectrum compared to the principle-based approach taken by the RBI. Critical sector entities however require specific guidance from the regulators on moving their workloads to the cloud and a risk-based approach that identifies workloads based on data classification and impact (Low, Moderate, High) based on NIST standards (FIPS 200, March 2006) would be a middle path to take, while revising the controls-based approach and harmonisation of regulatory framework.

Consultation should be an integral part of rule making

The nature of the cyber domain is that rule making cannot be divorced from implementation. With rapid digitisation, attack surfaces have increased exponentially. Hence check box approaches do not work and only create a sense of false security. Policy makers hence need to avoid suggesting prescriptive approaches and evaluate new models and frameworks based on evolving risks.

These models cannot however be evolved without extensive consultations with all parties concerned including CI entities, CSPs, Auditors, Standard bodies and other interested parties including Civil society organisations.

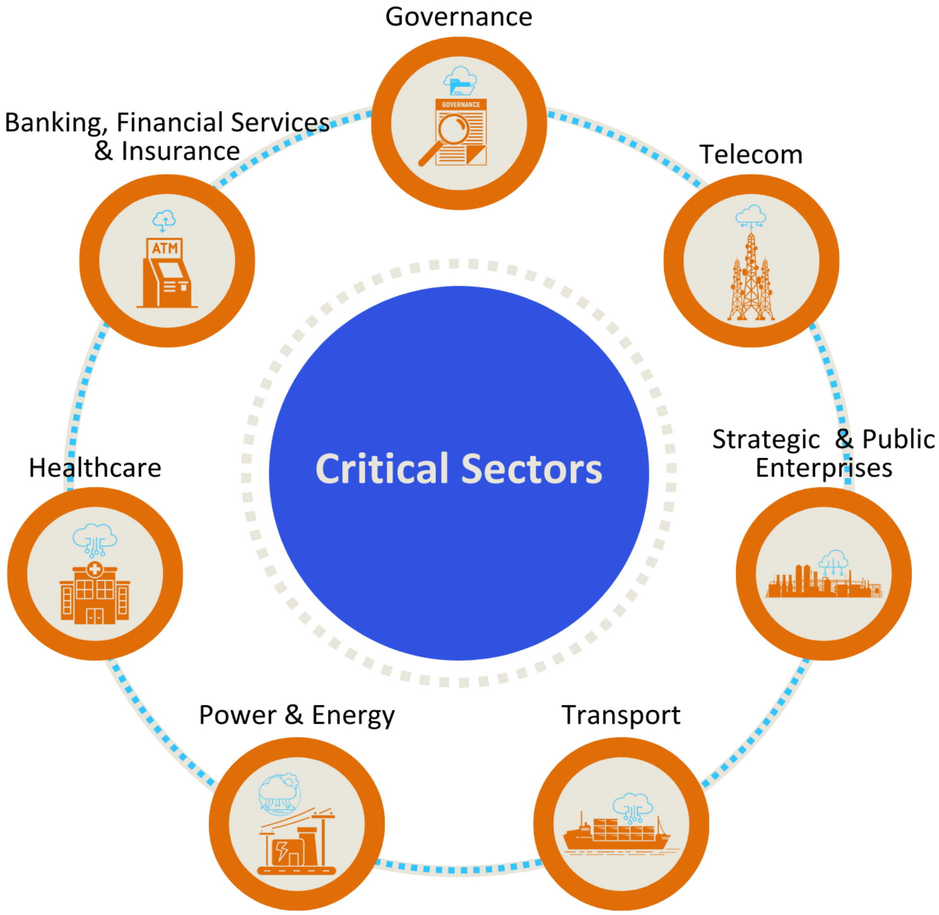
Capacity Building

Policy should acknowledge that CII entities will continue to use public cloud for various purposes, and provide enough guidance to those who chose this path, and should include:

- Pilot Projects, sandbox approach to build confidence for entities to experiment with cloud.
- Technical skilling of IT teams in emerging technologies and cyber security to bridge knowledge gaps.
- Training for Auditors in the cloud environment to address capacity constraints in the auditing field.

Adopt an evolutionary approach

A scan of several jurisdictions dealing with prescribing security for CSPs show various permutations and combinations that have their inherent strengths. From an Indian perspective, it is important to build a combination that works best for its CII sectors and its unique journey towards digitisation and subsequently, using cloud services. Japan is highly compliance-centric, which may not work for Indian conditions. However, for Indian policymakers, Germany's C5 model, as discussed in chapter 4 of this study reveals mature audit and update processes. In the US, a collaborative framework allows industry and the government to work together in a public-private framework.



8 Appendix A - Cloud Use Cases in Critical Sectors

Transport

California's Department of Motor Vehicles (DMV) carried out its digital transformation project with two partnerships – Azure[75] and AWS[76]. While the former is used for organising evidence centrally in a digital format with labelling, the latter was used for creating a customer connect experience to create bots that uses natural language processing to answer queries automatically. The virtual, cloud-based DMV also boasts an improved environmental impact, due to the elimination of paper and waste.

Government

In the Australian state of South Australia, the Department for Communities and Social Inclusion (DCSI) was able to deploy a single platform to automate contract administration and processing of payments to non-government organisations using a software-as-a-service cloud platform. This reduced payment processing time from 4–6 weeks to less than 3 days[77].

Telecom

XL Axiata is the second-largest telecommunications provider in Indonesia. In 2021, the company decided to adopt a hybrid cloud approach as part of its digital transformation and has adopted both AWS[78] and Google Cloud[79] with on-premises data centers to initiate employees into a cloud-based model.

Power and Energy

Cloud has also been the preferred solution for Portland General Electric (PGE), a regulated investor-owned utility that has operated in Portland, Oregon for 130 years and services 900,000 customers across 51 cities in the state. In 2021[80], it moved towards a data cloud architecture (Snowflake with AWS), which allowed users to access data through secure views, automate manual tasks and also a potential $1 Million of savings before the end of the year.

Global Power Synergy Public Company Limited (GPSC) Group is a front-runner in sustainable energy provision in Thailand[81]. In 2020, GPSC decided to migrate Glow Energy 2020, its newest acquisition at the time, to the public cloud. As a result, the Group has reduced operation costs by 20-25%, while ensuring data security and compliance. Its systems have also gained efficiency since migration to cloud also reduced load time for Windows applications by 20 seconds and removed the need to invest in hardware upgrade.

Banking and Finance

The SWIFT financial system is responsible for money transfer across 11,500 financial institutions spread world-wide. With the raise of instant payments, there is a need to do anomaly detection at scale to flag fraudulent transactions, but

[75] (Vidizmo, n.d.)
[76] (Government Technology, 2022)
[77] (Sales Force, n.d.)
[78] (Amazon Web Services, 2021)
[79] (XL Axiato, 2020)
[80] (SnowFlake, 2021)
[81] (Amazon Web Services, 2022)

without doing it all in one centralised location. With advances in secure edge computing, this was achieved via the Microsoft Azure cloud, which does anomaly detection at the edge and fuses the results in a foundational model[82].

[82] (Microsoft Corporation, 2023)

9 Appendix B - Audit Requirements of CII

NCIIPC's mandate includes evolving auditing methodologies and nurturing and developing audit and certification agencies for protection of CII. Its Standard Operating Procedure (SOP) of 2017[83] is used for auditing notified CIIs, Protected Systems, and those who are in the process of notification. An audit criterion has been established based on MHA Guidelines on classification of information. MHA classifies the impact of information's unauthorised disclosure into five categories - *top secret, secret, confidential, restricted, and unclassified.*

Top secret and Secret categories may have implications for national security or national interest, and therefore fall under Critical Segment Category – I of NCIIPC. A government auditor must conduct audit of this category. Confidential, restricted, and unclassified categories do not have implications for national security, and have, thus been classified as Critical Segment Category – II by NCIIPC. A private auditor may audit this category.

The organisations in critical sector must first classify their segments into the above two categories. After that, they are required to conduct an internal audit every six months. They also must conduct an annual external audit by a government or private auditor, based on the category a segment falls under.

A criterion for selection of auditors, based on their years of experience, has been provided. NCIIPC recommends that government auditors like STQC and those empanelled by CERT-In, be used to audit Critical Segment Category – I.

Harmonisation of baselines and a well-defined audit framework are necessary for achieving cadence among the various intersecting regulations. A step in this direction is the National Security Council Secretariat's latest "Cybersecurity Audit Baseline Requirements"[84] ("CSA-BR"). This document, developed in consultation with stakeholder regulators, aims to function as a minimum, common, harmonised baseline criterion for cybersecurity audits, and has been made mandatorily applicable for owners and regulators of CII. The CSA-BR also makes it the responsibility of CII organisations to themselves classify their risk profiles, unlike NCIIPC's SOP of 2017.

CII entities, however, bear the burden of classifying their networks, and meeting the audit requirements of each segment. This, because India has capacity constraints when it comes to trained technical experts and auditors for cloud, makes effective implementation of these requirements a hard problem.

India is faced with the problem of untrained auditors who are not equipped to audit cloud. The pace and method of training of auditors has not kept up with that of other countries. This problem is even graver in government auditors, who have been used to auditing legacy organisations. Their training in cybersecurity in cloud and their independence, are both causes of worry for the CIIs and CSPs.

Australia's proactive investment in enhancing IRAP policy and training, therefore, offers another valuable lesson for India. Especially since STQC certification is recommended, it is imperative for India to remove redundancies and ensure that its auditors remain familiar with developments and changes in relevant technology. Investing in revising and updating training curricula can provide assurance that auditors are adequately performing their roles and enhances the reliability of auditing systems.

[83] (NCIIPC, 2017)

[84] (National Security Council Secretariat, 2020)

10 Bibliography

Ministry of Law and Justice. (2009, February 9). The Information Technology Amendment Act 2008. Retrieved April 21, 2023, from The Gazette of India: https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf

Ministry of Electronics and Information Technology. (2014, January 16). IT Rules (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties). Retrieved April 13, 2023, from https://www.meity.gov.in/writereaddata/files/GSR_19%28E%29_0.pdf

NCIIPC. (2015). NCIIPC Guidelines V2. Retrieved from NCIIPC: https://www.nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf

Barik, S. (2022, December 10). Digital India bill to replace IT Act, 2000: . Retrieved from Indian Express: https://indianexpress.com/article/business/economy/digital-india-bill-to-replace-it-act-2000-govt-plans-classification-of-online-intermediaries-separate-norms-8316146/

Synergy Research. (2020, January 6). Cloud Goes from 0 to 100 in Ten Years while Enterprise Data Center Spending Stagnates. Retrieved from Synergy Research: https://www.srgresearch.com/articles/the-decades-megatrends-in-numbers-part-1

Clausewitz, C. V. (1873). On War.

US Marine Cops. (1989). FMFM1 Warfighting.

Joe, S. (1996). Centers of Gravity and Critical Vulnerabilities. Marine Corps War College.

The White House. (1998, May 22). PRESIDENTIAL DECISION DIRECTIVE/NSC-63. Retrieved from Presidential Decision Directives - PDD]: https://irp.fas.org/offdocs/pdd/pdd-63.htm

Humphreys, B. E. (2019, July 8). Critical Infrastructure: Emerging Trends and Policy Considerations for Congress. Retrieved from Congressional Research Service: https://www.everycrsreport.com/files/20190708_R45809_54416d7b2f43d41696e8e971832aea5fe96a9919.pdf

CISA. (2014, March). Critical 5, Forging a Common Understanding for Critical Infrastructure. Retrieved from CISA: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

Russian Federation. (2016, December 5). Doctrine of Information Security of the Russian Federation. Retrieved from http://www.scrf.gov.ru/security/information/DIB_engl/

Pursiainen, C. (2020). Russia's Critical Infrastructure Policy: What do we Know About it. European Journal for Security Research, 21 - 38.

Jong-Chen, J., & Brian, B. (2017, November). Wilson Center. Retrieved from https://www.wilsoncenter.org/sites/default/files/media/documents/publication/approach_to_critical_infrastructure_protection.pdf

Roberts, N. (2017). Wicked Problems and Network Approaches to Resolution. International Public Management Review., 3 to 7.

Center, National Cyber Security. (2018, November 17). The cloud security principles. Retrieved from https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

Barroso, L. A., & Hölzle, U. (2009). The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines. Morgan and Claypool.

Verma, A., Pedrosa, L., Korupolu, M. R., & Oppenheimer, D. (2015). Large-scale cluster management at Google with Borg. Proceedings of the European Conference on Computer Systems (EuroSys), ACM, 18.

Flake, H. (2020, September). ADD XOR ROL. Retrieved from http://addxorrol.blogspot.com/2020/07/the-missing-os.html

Amazon Web Services. (2021, June 2). Benefits of using multiple AWS accounts. Retrieved from https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/benefits-of-using-multiple-aws-accounts.html

Microsoft Azure. (2023, March 31). Organise and manage multiple Azure subscriptions. Retrieved from https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/organise-subscriptions

Amazon Web Services. (n.d.). Data Center Controls. Retrieved from https://aws.amazon.com/compliance/data-center/controls/

Microsoft Corporation. (2023, Februrary 13). Azure facilities, premises, and physical security. Retrieved from https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

MEITY. (2013). GI Cloud Meghraj. Retrieved from https://www.meity.gov.in/content/gi-cloud-meghraj

Republic Of Singapore. (2018, February 5). Cyber Security Act. Retrieved from Government Gazette: https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312#pr24-

Cyber Security Agency of Singapore. (2022, December 12). Cyber Security Act 2018. Retrieved from CYBERSECURITY CODE OF PRACTICE FOR CRITICAL INFORMATION INFRASTRUCTURE

Republic of Singapore. (n.d.). Singapore Standars Council. Retrieved from https://www.enterprisesg.gov.sg/grow-your-business/boost-capabilities/quality-and-standards/singapore-standards-council

Republic of Singapore. (n.d.). MTCS Certification Scheme. Retrieved from https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Compliance-and-Certification

The Government of Japan. (2020, October 13). The Basic Act on Cybersecurity (Act No. 104 of 2014). Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/2760#je_ch3at1

Onodera, Y., Tanaka, H., Tsuta, D., & Shimamura, N. (2023). 16GDR Insight Handbook 2023 Japan: Cybersecurity . Retrieved from Mori Hamada & Matsumoto: https://www.mhmjapan.com/content/files/00065821/20221104-110305.pdf

The Government of Japan. (2021, September 28). Cyber Security Strategy. Retrieved from https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf

The Government of Japan. (2022, June 17). The Cybersecurity Policy for Critical Infrastructure Protection. Retrieved from https://www.nisc.go.jp/eng/pdf/cip_policy_2022_eng.pdf

ISMAP Registration Committee. (2022, Novermber 1). ISMAP Cloud Service Registration Rules. Retrieved from https://www.ismap.go.jp/sys_attachment.do?sys_id=c6f7f210db0e65506e6cb915f396190d

ISMAC Steering Commitee . (2022, Novermber 1). Control Criteria of ISMAC. Retrieved from https://www.ismap.go.jp/csm/sys_attachment.do?sys_id=c6f7f210db0e65506e6cb915f3961909

The Australian Government. (2022, May 22). Security of Critical Infrastructure Act 2018. Retrieved from Federal Register of Legislation: https://www.legislation.gov.au/Details/C2022C00160/Html/Text#_Toc102382662

The Australian Government. (2022, March). Security Legislation Amendment (Critical Infrastructure Protection) Act 2022. Retrieved from https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-security-legislation-amendment-critical-infrastructure-protection-act-2022.pdf

The Government of Australia. (2022, July). Cyber Security Incident Reporting. Retrieved from https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cyber-security-incident-reporting.pdf

The Australian Government. (2023, January). Trusted Information Sharing Network. Retrieved from https://www.cisc.gov.au/engagement/trusted-information-sharing-network

The Australian Government. (2022, October). Secure Cloud Strategy. Retrieved from https://www.dta.gov.au/sites/default/files/2022-09/DTA%20Secure%20Cloud%20Strategy%20-%20October%202021%20v3.pdf

Brumsfield, C. (2019, July 1). What is the CISA? How the new federal agency protects critical infrastructure from cyber threats. Retrieved from CSO Online: https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html

Cybersecurity and Infrastructure Security Agency,. (2022, June). Cloud Security Technical Reference Architecture. Retrieved from https://www.cisa.gov/sites/default/files/publications/Cloud%2520Security%2520Technical%2520Reference%2520Architecture.pdf

Doubleday, J. (2022, March 25). From 'partner' to 'regulatory enforcer': CISA takes on complex cyber incident reporting mandate. Retrieved from Federal News Network: https://federalnewsnetwork.com/cybersecurity/2022/03/from-partner-to-regulatory-enforcer-cisa-takes-on-complex-cyber-incident-reporting-mandate/?readmore=1

CISA. (2022, March). Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) . Retrieved from CyberSecurity & Infrastructure Security Agency: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. (2004, February). Standards for Security Categorization of Federal Information and Information Systems. Retrieved from FIPS PUB 199: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

The United States Government. (2021, October 28). FedRAMP Market Place Designation for Cloud Service Providers. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

The United States Government. (2023, April 6). 3PAO Obligations and Performance Standards. Retrieved from FedRAMP: https://www.fedramp.gov/assets/resources/documents/3PAO_Obligations_and_Performance_Guide.pdf

Government of India. (2014, January 16). Information Technology Act Rules. Retrieved from

Gazette of India: https://www.meity.gov.in/writereaddata/files/GSR_19%28E%29_0.pdf

NCIIPC. (2019, August). Guidelines for CII Identification. Retrieved from Guidelines for CII Identification: https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf

Mitre Corporation. (2022, October). Attack Framework Revisions. Retrieved from Attack Framework: https://attack.mitre.org/resources/versions/

Federal Office for Information Security. (n.d.). Cloud Compliance Controls Catalogue. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf?__blob=publicationFile&v=3

Federal Office For Information Security. (n.d.). General Information on Kritis. Retrieved from What are Critical Infrastructures?: https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

OECD. (2019). Good Governance for Critical Infrastructure Resilience. Organisation for Economic Co-operation and Development. Retrieved from https://www.oecd.org/governance/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm

Vidizmo. (n.d.). DMV California takes disparate local evidence all over the state to manage centrally on VIDIZMO. Retrieved from Vidizmo: https://vidizmo.com/downloads/resources/case-studies/DMV-California-DEMS-Case-Study.pdf

Government Technology. (2022). How the California DMV implemented a faster, more customer-centered contact center. Retrieved from https://static1.squarespace.com/static/629f87965455bf40e553e50d/t/62cc8b9ae70401163176b50a/1657572250593/GT22_CASE_STUDY_AWS_CA_DMV_V.pdf

Sales Force. (n.d.). Salesforce drives DCSI service innovation to improve the lives of people with disabilities . Retrieved from Sales Force: https://www.salesforce.com/ap/customer-success-stories/dcsi/

Amazon Web Services. (2021). XL Axiata Transforms into a Cloud-First Telco with AWS. Retrieved from AWS Case Studies: https://aws.amazon.com/solutions/case-studies/xl-axiata-case-study/?did=cr_card&trk=cr_card

XL Axiato. (2020, June 9). XL Axiata Partners with Google Cloud to Advance Digital Transformation Strategy and Serve Customers in Indonesia. Retrieved from https://www.xlaxiata.co.id/en/news/partnership-xlaxiata-and-google-cloud

SnowFlake. (2021). Annual Cost Savings for Portland General Electric With the Snowflake Data Cloud. Retrieved from https://www.snowflake.com/en/resources/case-study/annual-cost-savings-for-portland-general-electric-with-the-snowflake-data-cloud/

Amazon Web Services. (2022). GPSC Group Migrates Windows Workloads to AWS to Reduce Costs and Optimize Performance. Retrieved from https://aws.amazon.com/solutions/case-studies/gpscgroup/?did=cr_card&trk=cr_card

Microsoft Corporation. (2023, May 23). Swift innovates with Azure confidential computing to help secure global financial transactions. Retrieved from https://customers.microsoft.com/en-in/story/1637929534319366070-swift-banking-capital-markets-azure-machine-learning

NCIIPC. (2017, June). STANDARD OPERATING PROCEDURE. Retrieved from https://nciipc.gov.in/documents/SOP-CII_Audit.pdf

National Security Council Secretariat. (2020, October). CYBER SECURITY AUDIT BASELINE REQUIREMENTS. Retrieved from https://nciipc.gov.in/documents/CyberSecurityAuditbaseline.pdf

DEEPSTRAT

STRATEGY . POLICY . ACTION

www.deepstrat.in