Gateway
Network
Governance
Body

Gateway Network Governance Body
contactus@gngb.com.au
www.gngb.com.au
31 August 2020

Cyber, Digital and Technology Policy Division
Department of Home Affairs
techpolicy@homeaffairs.gov.au

RE: GNGB submission to the Home Affairs call for views on Strengthening Australia's Cyber Security regulations and incentives

The Gateway Network Governance Body (GNGB) welcomes the opportunity to make this submission to the *Department of Home Affairs in relation regulations for strengthening Australia's Cyber Security environment*. GNGB is an industry-owned governance body which oversees the data infrastructure known as the Superannuation Transaction Network (STN) and has a key focus on cyber governance across the digital network. In early 2021 GNGB commissioned a report into the cybersecurity risks across the superannuation ecosystem, Securing the Future: Protecting Australia's superannuation ecosystem against cybersecurity threats, which has sparked an industry wide conversation on the calls to action. It is with this experience, GNGB provides this submission to the department's consultation paper. GNGB's response focuses on the STN and the broader superannuation context and is followed by an overview of GNGB and the STN.

Call for Views	GNGB Response
3. What are the strengths and limitations of Australia's current regulatory framework for cyber security? 4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?	✓ GNGB supports mandatory cyber security governance standards for large business, however any framework requires thoughtful implementation and should meet the following principles: ✓ Remove duplication with existing regulation – as mentioned in the department's discussion paper, industries such as financial services are already highly regulated across regulated entities. Any additional mandatory requirements should seek to complement and clarify existing regulation. A key finding of GNGB's Securing the Future report was that the regulatory framework for the superannuation industry is inconsistent and still maturing. Responsibility for governance of the Australian superannuation ecosystem is fragmented across multiple regulators with inconsistencies in how current standards are applied, together with the inefficiencies brought about by overlapping standards. 85% of respondents to our industry survey agreed that existing frameworks and standards should be aligned and streamlined. In addition to leveraging existing standards in place for already regulated sectors, GNGB supports the "top up" of non-regulated entities with a standardised baseline. ✓ Dependencies exists between organisations within the digital economy. As outlined in GNGB's Securing the Future report, the dependencies between organisations within the digital environment present opportunities for exploitation of weak security controls. Specifically, within the superannuation ecosystem, our report found that over 1.5M

Call for Views	GNGB Response
	organisations are responsible for managing or storing superannuation fund member data. See diagram 1. The confidentiality, integrity, and availability of that data rests with each of those individual organisations. It is to be expected, and in line with our report findings, that there are varying degrees of maturity in managing the protection of that data along the supply chain. As a result, we believe mandatory standards for all large organisations with a responsibility to protect consumer data, in an appropriate way, is the preferred approach. In addition, a baseline of security standards for small to medium organisations is also required, due to the dependencies created by digital integration. ✓ Options for enforcement may vary based on risk and range from self-attestation to independently accredited compliance. For example larger organisations may be required to demonstrate compliance and smaller organisations able to complete a self-assessment. ✓ What is appropriate? Consultation and co-development with industry is required on what should constitute mandatory standards for large organisations and baseline of security standards for small to medium organisations. The GNGB information security standards provide an example of the successful co-design between industry and the regulator of agreed standards, with an ongoing high level of engagement and compliance, as well as continuous improvement to ensure the standards meet changing and evolving security needs. Whilst the STN security standards are designed specifically with the STN in mind, they are aligned with similar industry standards for example the government's Information Security Manual (ISM), ATO's Operational Security Framework and APRA's CPS234 and incorporate elements of internationally recognised standards such as ISO27001. ✓ There are many existing security standards today that have been developed with a specific purpose or objective in mind, however GNGB would support a common baseline of a security standards such as the government's essential eight controls across all organisations as a minimum. The essential eight maturity framework has the benefit of enabling compliance for a variety of organisational sizes and capabilities. Those organisations already regulated with regard to cyber security would likely already cover or be working towards the essential eight's key themes, and those that do not would now be required to implement a minimum baseline of protection resulting in a uniform uplift in resilience. ✓ A mandatory approach has the following benefits: ● Provides impetus for decision making and investment into cyber security ● Clarifies liability and Board responsibilities of information security ● Prioritises education and up-skilling building resilience capability across all

Call for Views	GNGB Response
8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?	✓ GNGB does not consider that a cyber security code under the Privacy Act would be an effective way to promote the uptake of cyber security standards in Australia. ✓ The Privacy Act mainly deals with Personally Identifiable Data (PII) and while inclusion of a cyber security code or similar into the Privacy Act might provide strengthened protection of PII, it would not necessarily provide protection of other types of data, such as commercial data. ✓ Increasingly software and operational technology vulnerabilities are being exploited with the purpose of disruption and destruction rather than unauthorised access to data. Examples include the increasing attacks on logistics, supply chain, energy and food assets. In addition, examples of unauthorised access to an organisation's intellectual property, rather than PII, are increasing in frequency and consequence. Any minimum standard should seek to cover the risks of operational technology disruption and protection of critical data to the operation of an organisation, in addition to unauthorised access to personal information. ✓ A further limitation of including the cyber security code in the Privacy Act, is that the Act currently only applies to organisations with revenue of greater than $3 million per annum. Should the government determine to incorporate a cyber security code or similar into the Privacy Act, it would need to ensure that the standardised requirements or code applies to all organisations, not just those organisations greater than $3M revenue currently covered by the Act. ✓ In addition, some states, particularly NSW, Victoria and the ACT have state-based privacy legislation that exists in addition to the *Privacy Act 1988 (Cth)*. This creates confusion and duplication. Any changes would need to consider the implications for those entities covered by both Commonwealth and state regimes. ✓ A cyber security code or minimum standard needs to be more broadly applicable than the current Privacy Act settings, noting that there is a proposed review of the Privacy Act underway Review of the Privacy Act 1988 | Attorney-General's Department (ag.gov.au). ✓ It is critical that the building of cyber resilience and protection of personal information occur in a risk based, efficient and sustainable way to maximise benefits for all organisations. For this reason, GNGB believes a broad-based hierarchy of frameworks across the digital economy may be the best approach. See proposed framework Diagram 2 which outlines a cyber security governance approach that: ● Identifies a single body for the overseeing of cyber security regulation across the economy. ● Includes a comprehensive, single framework of requirements appropriate for the different needs and proportionate to the

Call for Views	GNGB Response
	different risks, of each economy sector or role an entity plays within the economy. ● Seeks to “top up” those entities that are currently unregulated, whilst simplifying the regulatory landscape of those that are already regulated by acknowledging, validating and streamlining current regulatory accountabilities, and supplementing those that are partially captured under existing regulations. ● Develops a single source of truth for cyber security strategy, operational obligations and enforcement, for Australian businesses and individuals.

GNGB welcomes further dialogue in relation to Home Affairs consultation, please do not hesitate to contact us for further information.

Kind Regards

contactus@gngb.com.au

Diagram 1

Superannuation ecosystem

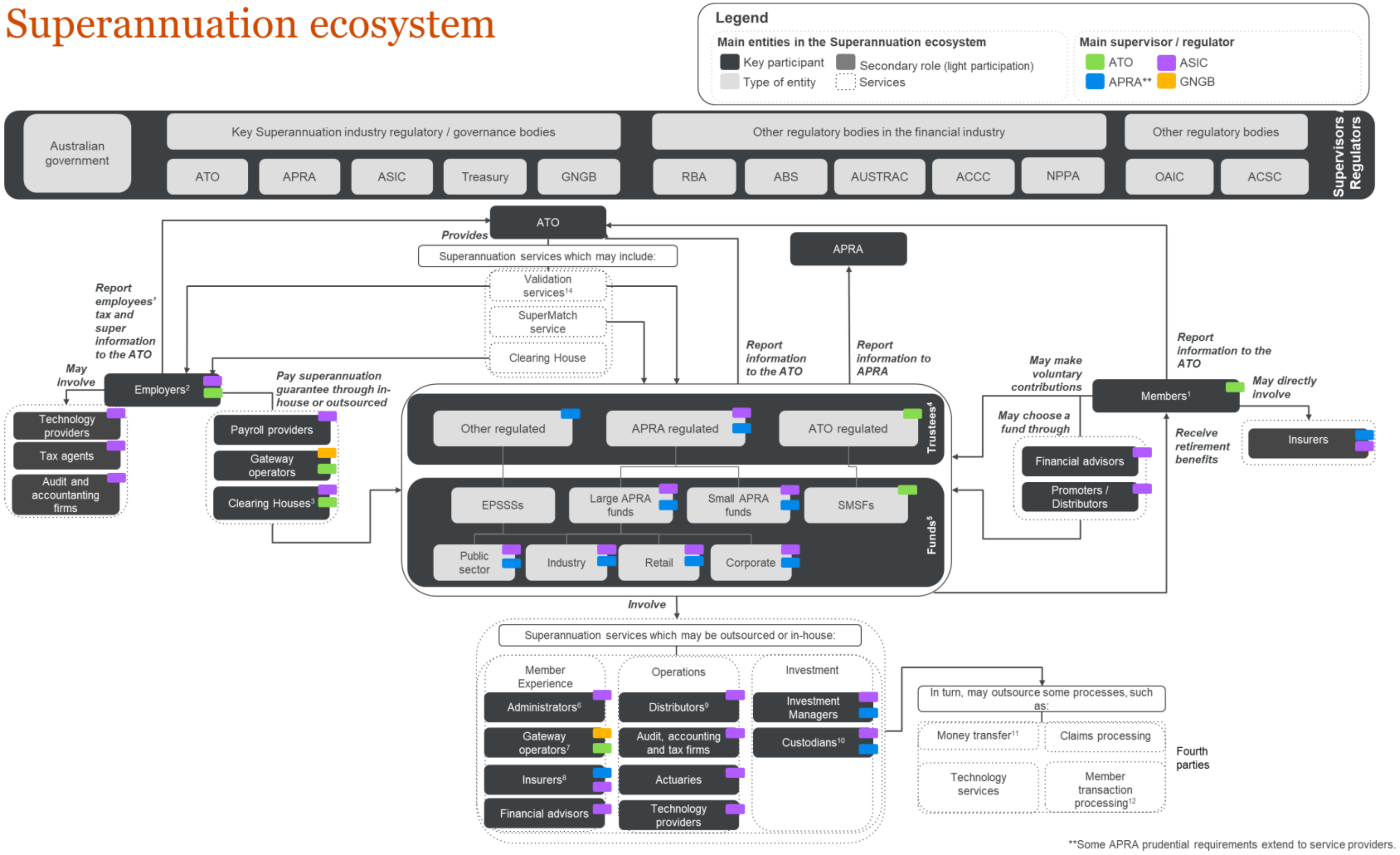
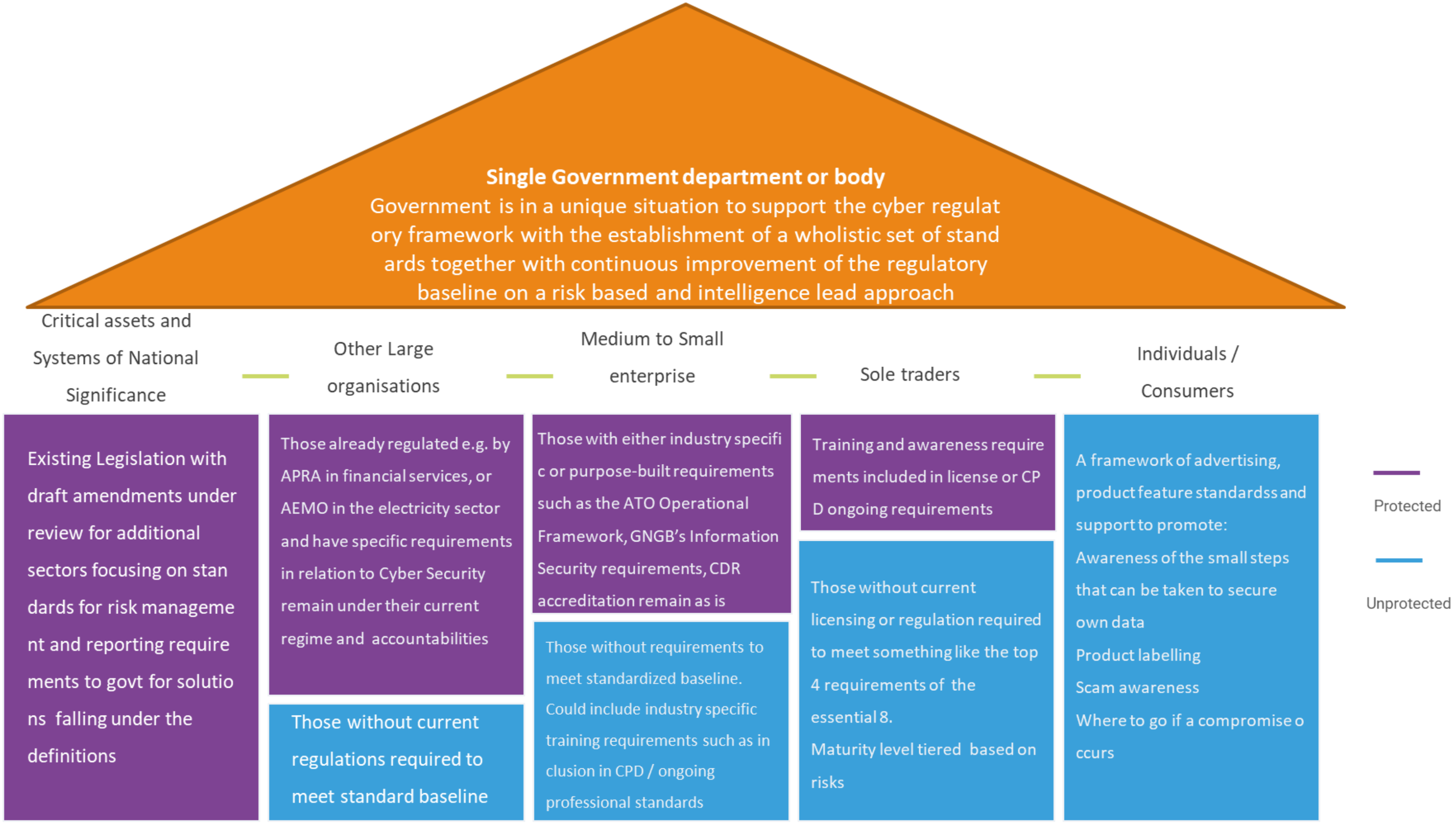


Diagram 1 outlines the complexity of the superannuation ecosystem and its regulatory environment. Coloured squares on each entity designates its main regulator(s) which in a large number of cases is ASIC in relation to Corporate Governance. ASIC cyber security objectives are largely currently met via the enforcement of Director accountabilities and duties.

Diagram 2

Outlines an example of a whole of economy approach to enabling a secure baseline whilst acknowledging existing cyber security requirements in place today.



Single Government department or body

Government is in a unique situation to support the cyber regulatory framework with the establishment of a wholistic set of standards together with continuous improvement of the regulatory baseline on a risk based and intelligence lead approach

Critical assets and Systems of National Significance

Existing Legislation with draft amendments under review for additional sectors focusing on standards for risk management and reporting requirements to govt for solutions falling under the definitions

Other Large organisations

Those already regulated e.g. by APRA in financial services, or AEMO in the electricity sector and have specific requirements in relation to Cyber Security remain under their current regime and accountabilities

Those without current regulations required to meet standard baseline

Medium to Small enterprise

Those with either industry specific or purpose-built requirements such as the ATO Operational Framework, GNGB's Information Security requirements, CDR accreditation remain as is

Those without requirements to meet standardized baseline. Could include industry specific training requirements such as inclusion in CPD / ongoing professional standards

Sole traders

Training and awareness requirements included in license or CPD ongoing requirements

Those without current licensing or regulation required to meet something like the top 4 requirements of the essential 8.
Maturity level tiered based on risks

Individuals / Consumers

A framework of advertising, product feature standardss and support to promote:
Awareness of the small steps that can be taken to secure own data
Product labelling
Scam awareness
Where to go if a compromise occurs

🟪 Protected

🟦 Unprotected

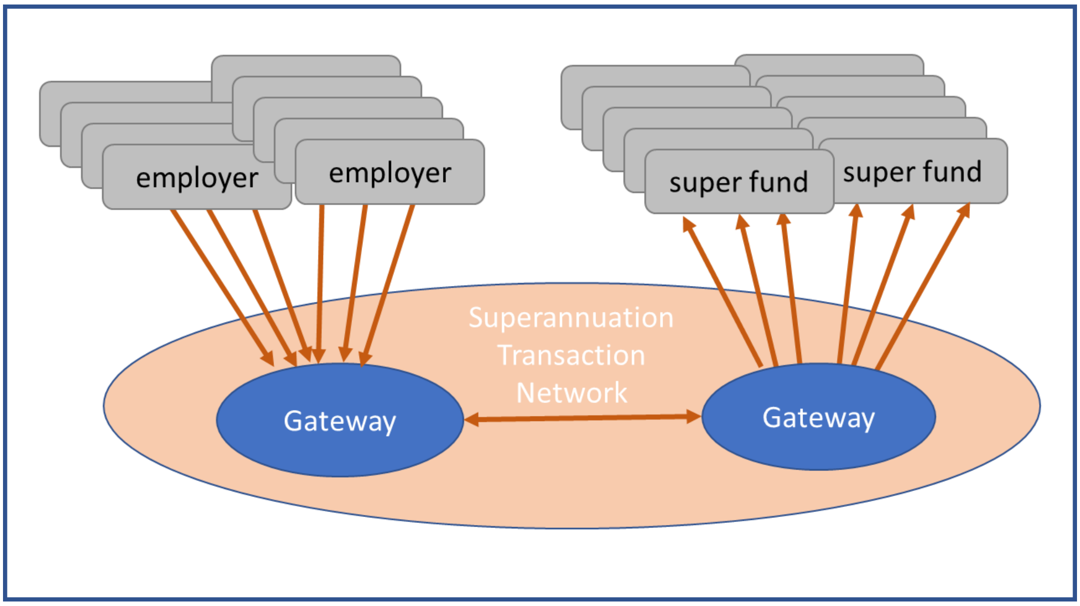
About us

The Gateway Network Governance Body Ltd (GNGB) was established in 2016 as an industry owned, not-for-profit governance organisation whose main purpose is to manage the security and integrity of the Superannuation Transaction Network (STN).

The STN is the data infrastructure that connects employers to the superannuation funds of their employees. It is the digital data messaging network over which superannuation transactions, such as rollovers and contributions, are sent between employers and funds via their technology service providers, who are known as Gateway Operators. The STN is currently connected to all Australian Prudential Regulation Authority (APRA) regulated superannuation funds and will incorporate Self-Managed Superannuation Funds (SMSFs) from March 2021. Since July 2018, over 694,000 employers have transacted over the network with an average of approximately 83 million data transactions per year. There are currently nine Gateway Operators within the STN. Since 2016, GNGB has been successful in the implementation of governance across the STN, specifically:

- Undertaking initiatives to promote the security, **efficiency and effectiveness** of the STN
- **Monitoring compliance** with the Gateway Standards, together with developing and providing oversight of specific Information Security Requirements
- Managing **new entrants and exiting gateway operators** to the network
- **Engaging with key stakeholders** in Government and industry
- Coordinating **change management** activities as legislation and associated instruments change, including the facilitation of member forums and opportunities to test and validate interpretation of legislative change, emerging technology and other developments.

It is important to note that the STN is defined by the boundaries around which Gateway Operators interact with each other, in relation to current governance scope. The STN is a four corner model of data exchange, with the STN Governance framework coverage extending across corners two and three. The below diagram outlines scope of the current regime in the example of contributions messages:



GNGB Stakeholders

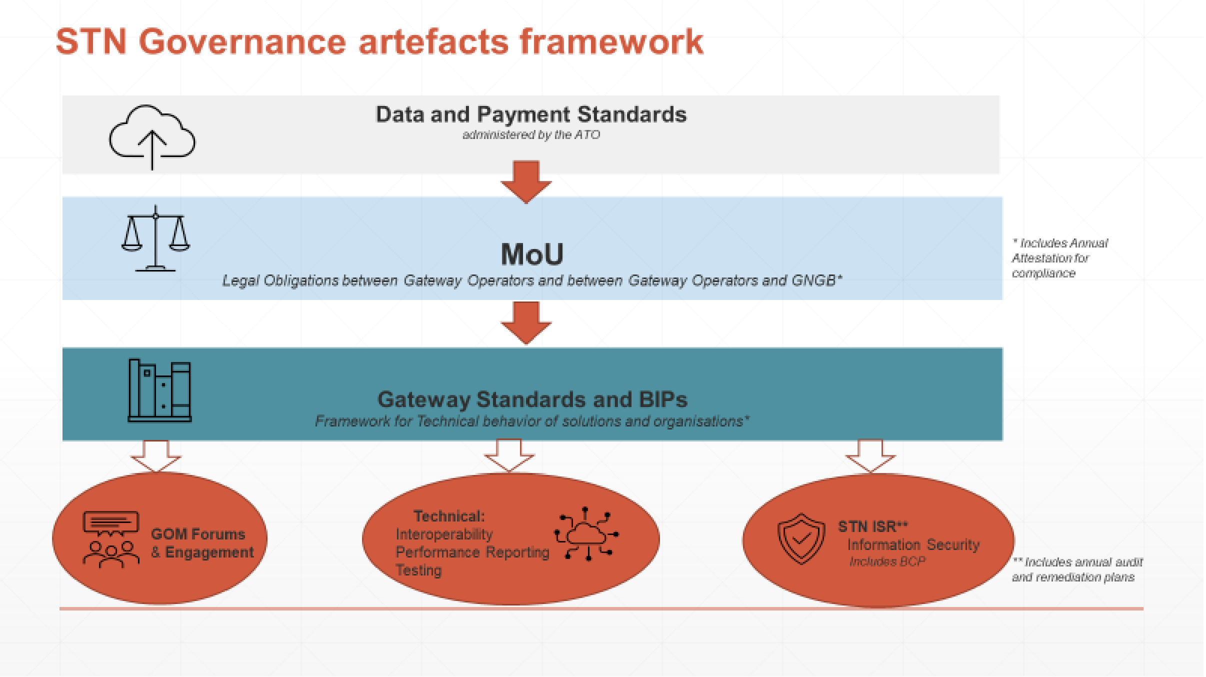
The accredited Gateway Operators within the STN range from large bank supported organisations or subsidiaries, to small business operators and fintechs. GNGB is experienced in guiding organisations across the maturity spectrum to identify, develop and implement solutions within a highly regulated environment.

In addition, GNGB's co-sponsor members (i.e. the founders of the organisation) are involved in the design and development of GNGB and are also represented on the GNGB Board. Co-sponsor members include:

- ABSIA – Australian Business Industry Software Association
- ACCI – Australian Chamber of Commerce and Industry
- AIST – Australian Institute of Superannuation Trustees
- ASFA – The Association for Superannuation Funds of Australia
- FSC – Financial Services Council

Current STN Governance Framework

The current governance framework consists of an MoU binding Gateway Operators to each other and to GNGB in respect of their obligations. The MoU outlines compliance with Gateway Standards (framework for interacting) and Information Security Requirements (STN ISR), largely based on the government's information security manual controls.



STN Governance artefacts framework

Data and Payment Standards
administered by the ATO

MoU
*Legal Obligations between Gateway Operators and between Gateway Operators and GNGB**

** Includes Annual Attestation for compliance*

Gateway Standards and BIPs
*Framework for Technical behavior of solutions and organisations**

GOM Forums & Engagement

Technical:
Interoperability
Performance Reporting
Testing

STN ISR**
Information Security
Includes BCP

*** Includes annual audit and remediation plans*