Digital Government Blueprint 2.0

With the culmination of the first Digital Government Blueprint (2018 – 2023), SNDGG is refreshing the objectives and strategies for the next bound of Digital Government (working name: Digital Government Blueprint 2.0 (DGB 2.0)). This paper proposes the key strategic thrusts for DGB2.0, taking into account the progress we've made so far as well as potential derailers and new opportunities.

Progress of Digital Government

2. Under the first Digital Government Blueprint (DGB 1.0), we have **digitalised Government services and achieved high citizen and business satisfaction**. Products such as Singpass, PayNow and FormSG have gained high traction with the public and public officers. We have also **laid a good baseline of central ICT infrastructure**, including enabling cross-agency data sharing and successfully shifting our systems to cloud. This was possible because we **re-built ICT&SS capabilities within Government**, reversing earlier years of out-sourcing. Through the Ministry Family Digitalisation Plans, we have also observed an increase in digital ambition from the Ministry Families. These efforts were key to Singapore's rapid digital response to COVID-19, and have supported Singapore's global standing as a leading Digital Government. More details on the indicators for DGB 1.0 can be found in Annex A.

Impetus for Change

3. There is much more that we can do to fully leverage digital technology as a transformative force. For example, Ministry Family Digitalisation Plans reflect that Ministry Families tend to focus their digital transformation efforts on optimising existing processes, rather than more fundamentally changing business models. Additionally, there are new derailers and opportunities for digitalisation, even as Government faces even sharper constraints than when the first Blueprint was developed.

a) Externally, there are growing concerns about digital inclusion and digital trust and safety. 52% of respondents to MCI's 2022 Public Perceptions Towards Scams in Singapore survey are moderately or extremely concerned that they will fall prey to scams. While this is partly a result of how we have extensively digitalised services, these concerns can lead to stronger public resistance towards digitalisation, potentially even derailing our broader Smart Nation efforts.

b) Internally, Government also faces a few key challenges:

i) Today, **many ICT systems across Whole-of-Government (WOG) are old, obsolete, and poorly designed ("legacy")**. As a proxy, there are about 370 Government systems which are more than 10 years old, with this number set to double in the next 5 years. These hinder our digital ambitions and pose risks to our operations and service delivery, creating a negative public experience (e.g. long waiting times to enter HDB's BTO portal, ICA's checkpoint disruption).

ii) **Our digital capabilities are still insufficient**. We continue to see poorly-designed and costly digital systems and products across agencies, and also **need to improve our vendor ecosystem** in light of WOG workforce constraints. For example, and agency had initially proposed a platform which would have cost over $100m over five years. SNDGG helped to simplify their proposal and clearly identify the problem statement, and the agency eventually started with a pilot of $0.9m. Another agency similarly proposed a vendor-built bespoke system which would cost $104m over 5 years, but after SNDGG's intervention, was able to pivot their proposal to tap on a SaaS solution to meet most of their needs for about 40% of the initial cost.

iii) We **need to improve the digital workplace experience of public officers**. While we have made significant progress in this area (e.g. smooth transition to work-from-home and hybrid arrangements during COVID-19), the day-to-day IT experience of public officers is still far from that in modern companies (e.g. the average time taken to access emails/ other applications from laptop start-up is at least 5 – 10 minutes, and can be reduced to less than 1 minute.

c) There are also new opportunities which have arisen:

i) **Artificial Intelligence is a potential game-changer for employee productivity and service delivery**. Substantial effort is needed to harness its potential, which can also support our international positioning as a leading Digital Government.

ii) We should also **fully exploit our shift to Cloud, to enable greater use of Software-as-a-Service (SaaS)**.

d) We also face sharper constraints. Beyond the WOG **manpower and fiscal constraints, carbon constraints are now more pertinent** and under greater public scrutiny.

Digital Government Blueprint 2.0: The Way Forward

4. Given this context, Government will need to make key shifts to **improve the experience of our citizens (Thrust 1) and employees (Thrust 2)**. This will address the derailers, and also maintain the momentum and confidence in our digital government efforts. To achieve this, we need to **significantly uplift our digital capabilities (Thrust 3) and put in place the right enablers (Thrust 4)**. These will **support agencies in leveraging digital technology for deeper and bolder transformation.** Finally, given sharper constraints, we will **put in place measures to maximise the use of our available resources** (Thrust 5).

Thrust 1: Ensure that all Singaporeans can trust Government services and find them easy to access and use

5. Digital transformation should ultimately enhance citizens' lives and enable Government to better serve the public. We will work with ServiceSG to continue to **integrate services around citizen needs, and identify key service bundles to transform over the next five years**, based on citizen archetypes which have more interaction with Government (e.g. parents, low income and vulnerable groups, seniors etc.). The Government must **design its services with greater inclusion in mind** (i.e. well-designed digital services that even the less digitally-proficient find easy to use; providing support for digital services and non-digital options). We will **put in place the tech enablers to support these efforts** (e.g. to enable better case coordination across agencies), and deliberately create opportunities to **co-create digital solutions with the public**[1].

6. We also need to **improve the security and resilience of Government systems and services**, given the fast-evolving threats in the digital space. In particular, we need to enhance trust and safety by **allowing citizens to identify genuine Government messages and transactions** so they can transact with peace of mind.

Thrust 2: Significantly improve the workplace experience of public officers

7. We can do a lot more to **enhance the public officer's day-to-day IT experience and enable their work with digital tools**. The credibility of Government digital transformation is undermined if our own officers do not see it manifested in their everyday work. Our on-going work to separate the Secret network will allow for **greater adoption of SaaS for non-Secret users** and enable us to raise the baseline suite of non-S applications across WOG (e.g. from SG-Teams and Workday today).

[1] In June 2022, SNDGG launched 'Build for Good', an inaugural citizen hackathon reflecting a new modality of citizen engagement and empowerment. The initiative empowers citizens to contribute and lead the change to make Singapore better.

8. We are also **developing a suite of Government Artificial Intelligence (AI) products to deliver 10x productivity gains and improve service delivery in core and/or common areas of public sector work**. These include productivity tools to help officers analyse and draft replies to Parliamentary Questions, and service delivery products to recommend Government support schemes. To fully realise the impact of such AI-powered tools, we also need to **ensure accessibility and raise proficiency in their use**.

Thrust 3: Uplift digital capabilities and competencies to enable deeper and bolder transformation

9. **Strong digital capabilities and competencies are fundamental to achieving Government's digital ambitions and enabling deeper and bolder transformation.** If we do not strengthen capabilities, we will continue to see poorly designed products that are too costly and slow to market. Within Government, there are four key areas to develop:

a) First, we will need to work with PSD to **significantly enhance the 'tech quotient' of 'game-changers' and decision-makers (e.g. Public Service Leaders, Directors)**. These individuals set the ambition for digital transformation in their respective areas, and have the authority to create structures and processes to ensure policy-ops-tech integration. Deeper and bolder transformation will be difficult to achieve without strong leadership. In addition, we will raise the broad-based capabilities of MX Officers (i.e. MX13 and above) to exploit digital tools and AI to improve their personal and organisational productivity at work.

b) To support this first group, we need to **continue to raise-train-sustain a highly competent WOG ICT&SS workforce**, with a focus on strong competencies given manpower constraints. We will also **continue to build central capabilities in core technical domains** such as software engineering, product and design, cybersecurity, data science and cyber-physical interfaces.

c) Third, we will also make a **concerted push on building up deep AI capabilities to seize opportunities in this area**. While the space is constantly evolving, we will keep pace by developing capabilities to adapt foundational models for enterprise use by Government agencies. This includes fine-tuning and querying internal data bases for sectoral/vertical use cases, and model deployment. We will also look to partner industry to explore problem statements and enable capability transfer.

d) Finally, beyond building central capabilities, SNDGG will also review how GovTech supports WOG needs. There will be a **greater push towards forward deployment to support agencies more directly**, especially in key areas such as product development and management.

10. The vendor ecosystem is also an important stakeholder as they deliver a significant proportion of our ICT&SS projects. Experiences such as the challenging rollout of the Human Resource Payroll System show a clear need for us to uplift the vendor ecosystem. We will need to redouble efforts to **strengthen strategic partners and support their efforts to deepen capabilities and competencies.**

Thrust 4: Strengthen enablers for agencies to fully leverage digital technology to enable deeper and bolder transformation

11. Beyond digital capabilities, we also need to put in place other enablers (and remove barriers) to enable agencies' digital transformation. First, we will **make a substantial move to modernise Government legacy systems**. These systems are costly to operate, less resilient, and also difficult to integrate with new systems. Given limited central resources, we will need to prioritise key systems, and extract and propagate the success factors to other agencies.

12. Second, while we have made substantial progress in data-sharing for policy making, we can do more to **boost data-driven operations and service delivery and strengthen data culture across Government**. Emerging data technologies enable us to **significantly improve data discoverability across Government**, while the modernisation effort provides an opportunity to create **more API-enabled data sharing**. Effective use of data will also require us to continue **building officers' capabilities in data exploitation while increasing investments in data management and engineering capabilities**.

13. Third, we will also need to **change how we approach ICT&SS policy and governance**. Some policies are already outdated for today's technologies, or overly-prescriptive. SNDGG's effectiveness in policies, processes and standards is one of its lower performing areas (70% satisfaction amongst agencies in 2022). This increases the compliance burden and hinders innovation. We will have to **take a more flexible and tiered approach**, which will help to facilitate the adoption of SaaS and emerging technologies.

Thrust 5: Maximise use of our available resources

14. Given the larger manpower constraints, SNDGG will work with PSD to **identify to a sustainable manpower trajectory for the WOG ICT&SS workforce**. SNDGG will also continue to **push for central, reusable products** for better cost-effectiveness (see box story below), **support agencies in right-sizing their projects** (e.g. via Tech Panel[2] and Public Sector Infocomm Review Committee), and **help agencies leverage on SaaS opportunities** to reduce development costs.

Improving engineering productivity through central, reusable tools/ platforms

SNDGG has developed a central suite of tools/platforms for developers to develop good, reliable, and secure products more quickly. We embarked on our Cloud journey in 2018 with the Government on Commercial Cloud (GCC) initiative – a central platform for migrating Government services onto Cloud. This shift to Cloud facilitated our rapid digital response to COVID-19. A 2021 study on 13 Cloud-migrated Government systems also showed savings of between 27% and 42% in ICT operating costs. We have continually upgraded our central platform, significantly reducing onboarding time for developers to less than a day while maintaining compliance to security requirements. Currently, we are on track to meet the DGB 1.0 KPI of migrating 70% of eligible Government systems to commercial Cloud by end-2023.

SNDGG has continued to enhance the Singapore Government Tech Stack (SGTS) which streamlines and simplifies software development processes and productivity through (i) common development tools to enable consistent bespoke system development by public officers and vendors (i.e. Secure Hybrid Integration Pipeline Hive Agile Testing Solutions (SHIP-HATS) toolchain) (ii) reusable components to support common tasks (e.g. payments, bookings) and (iii) StackOps monitoring tool to enable full-service monitoring for better system resiliency.

15. We will also study how to **improve the environmental sustainability of Government ICT&SS**. Beyond consolidating government data centres, we will need to explore other opportunities such as green procurement and disposal of Government IT equipment.

16. An overview of the key initiatives in DGB 2.0 under the 5 thrusts can be found in Annex B.

Next Steps

[2] SNDGO introduced a Tech Panel under PSIRC in Nov 2022 to provide advice on more cost-effective technical solutioning approaches for projects that are complex and/or have high resource asks.

17. We are developing indicators to track the next bound of Digital Government and similar to the first DGB, will make some of these KPIs public to signal our next bound ambition.

18. Considering the widespread impact of digital technology across all areas of government, DGB2.0 will need to be a whole-of-government effort. SNDGG has worked with ServiceSG to complete engagements with Service Council members, Quality Service Managers community and selected PSes to validate our strategies. Moving forward, we will continue our engagements within Government, including with Chief Digital Strategy Officers, Chief Data Officers and Chief Information Officers. SNDGG will also continue to plan for more engagements with citizens, businesses and public officers.

For Discussion

19. SNDGG's proposed approach to DGB2.0 is submitted for information, please.

Prepared by : SNDGG

Annexes
Annex A – Digital Government Blueprint 1.0 Key Performance Indicators
Annex B – Key Digital Government Blueprint 2.0 initiatives

Annex A – Digital Government Blueprint 1.0 Key Performance Indicators (Prelim CY2022)

Category	*DGB KPI*	*Target*	*2022[1]*	*2021*	*2020*	*2019*	*2018*
Stakeholder Satisfaction	**KPI 1: G2C Satisfaction**	75%	84%	85%	85%	86%	78%
	KPI 2: G2B Satisfaction	75%	79%	76%	76%	77%	69%
	KPI 16: G2E Satisfaction	75%	83%	72%	79%	71%	50%
End-to-End Digital Options[2]	**KPI 3: 100% of services that offer e-payment options**	100%	99%	98%	96%	90%	81%
	KPI 4: 100% of services that are pre-filled with Government-verified data	100%	90%	75%	59%	54%	37%
	KPI 5: 100% of services that offer digital options for wet ink signatures	100%	94%	83%	72%	61%	42%
End-to-End Digital Transactions[2]	**KPI 6: 90-95% of transactions completed digitally from end to end**	90-95%	99%	99%	97%	96%	87%
	KPI 7: 100% of payments via e-payment[3]	100%	99%	99%	98%	96%	95%
Transformative, AI and data Analytics (DA) projects	**KPI 10: Transformative Projects[4]**	30-50	>50	50	60	44	18
	KPI 11: Ministry Families with high impact AI[5] projects (1 high impact AI project by 2022, 2 by 2023)	100%	17/20	16/20	20/20[6]	20/20[6]	20/20[6]
	KPI 12a: High impact data analytics cross-agency projects	15	20	10	15	9	4
	KPI 12b: MFs with at least 2 high impact data analytics projects	100%	15/20	15/20	15/20	14/20	10/20
Digital Capabilities	KPI 8: 40% of required officers in every agency with the requisite data literacy (80% of required officers in every agency in 2023)[7]	100%	86%	70%	45%	No data	
	KPI 9: 100% of public officers who require basic digital literacy training to be trained	100%	100%	99%	>95%	No data	
Data	**KPI 13: Government data that follow stipulated machine-readable standards on SG-DRM**	100%	100%	100%	100%	100%	N/A
	KPI 14: 7 working days to share core data for inter-agency data science projects (incl fusing)	100%	99%	98%	98%	No data	
Commercial Cloud Migration	**KPI 15: 70% of eligible Government systems on commercial cloud**	70%	67%[8]	55%	38%	No data	
Security	KPI 17: No major incidents[9] on Government-owned ICT&SS[10] CIIs	0	0	0	0	0	0
	KPI 18: Median time needed from incident[11] intrusion to containment	<13 Days	3.11	3.24	4.21	4.5	13.63
	KPI 19: Time from incident intrusion[12] to containment of 90th percentile of incidents	<230 Days	970.83	37.85	25.44	151.38	286.85

Legend: Green – target met; Orange – on track; Red – target at risk; Bold – public KPIs

Notes

1. DGB 1.0 KPIs for CY22 are being currently being collated and figures may not be final.
2. KPIs 3 to 7 exclude services where the KPI cannot be met for valid reasons (e.g. legislative reasons, or that certain population segments are unable to have access or use digital tools).
3. SNDGG had assessed that at this juncture, it is neither necessary nor desirable to hit 100%, and that maintaining non-digital payment options ensures inclusivity for citizens and businesses. Nonetheless, SNDGG will continue to ensure that all Government services provide at least one remote e-payment option by 2023.
4. SNDGG tightened the criteria for transformative projects to only include projects in the development or operational phase, as those in the earlier phases might face a higher risk of not meeting the 2023 deadline. This resulted in a reduction of projects reported for this KPI from 2020.
5. SNDGG tightened the criteria to high-impact projects (i.e. (i) the project has been implemented, and impact has been measured; (ii) the project has a high impact in terms of cost and time savings, enhanced performance, improvement in business or operational processes and/or refined existing policies; or (iii) the project has a sufficiently wide scope to improve agency’s core business goals or is mission critical).
6. Based on earlier KPI of ‘percentage of Ministry families that use AI for service delivery or policy making’.
7. The publicly-committed KPI is for 20,000 public officers to be trained in data analytics and data science, which has been met
8. As of June 2023.
9. Major incidents refer to incidents that lead to service disruption, compromise of sensitive information or integrity of CIIs. The definition is based on CSA’s National Cyber Incident Response Framework. When referenced to GITSIR's 5 scale severity rating, it would be medium and above severity rating.
10. This KPI does not cover CII-Operational Tech systems.
11. All incidents that involve system intrusions or data breaches.
12. There were 3 incidents that took more than 230 days to discover and have significantly skewed the data: (1) Malware infection on SPS non-GSIB workstation, (2) Malware infection in SPF Workstation and Removable Storage Media, (3) Potential data leak on CSC Learn app. The Malware infections were left undiscovered since 2018 on isolated agency-managed workstations using outdated anti-virus software.

Annex B – Key Digital Government Blueprint 2.0 initiatives

We have listed the key initiatives under the 5 DGB 2.0 thrusts in the table below. The initiatives are at varying stages of development, and SNDGG will continue to work with agencies to flesh out the strategies and plans prior to the launch of DGB 2.0.

S/N	Initiatives
Thrust 1: Ensure that all Singaporeans can trust Government services and find them easy to access and use	
1.	Government digital services which are more seamless, discoverable and personalised Under the first DGB, we have attained high citizen satisfaction with our Government-to-citizen digital services. However, there is still room to improve (e.g. survey feedback indicates that Government services could be more seamless, with respondents expressing dissatisfaction about needing interactions with multiple agencies to resolve their issue). A key deliverable under this initiative is ServiceSG and SNDGG identifying a list of key services to transform over the next 5 years, based on citizen archetypes which have more interaction with Govt (e.g. parents, low income and vulnerable groups, seniors etc.). The intent is to make these services much more discoverable, seamless across different touchpoints/ agencies and simple to apply for. ServiceSG is also working with SNDGG to identify and develop the necessary systems and data pipelines to enable this next bound of service delivery (e.g. Recommender & Personalisation Engine to power personalised service offerings). To improve the inclusivity of our digital services, SNDGG will refresh the Digital Service Standards to be explicit about digital design standards for seniors/vulnerable persons, and step up user testing with representative user groups. ServiceSG will also put in place assistance plans for seniors or the less digitally savvy (e.g. enabling trusted persons to perform transactions). Finally, the ServiceSG centres remain as a physical channel for those who are unable to transact digitally.
2.	Trusted and secure communications and transactions with the Government Public trust in Government digital communication has been eroded by the continued rise in phishing scam cases that impersonate government agencies. Our current measures to help members of public (MOPs) identify Government communications is not sufficient; some MOPs are turning away public officers reaching out to them. SNDGG is therefore studying the creation of a secure, trusted network of Government communications where MOPs can trust what they received from verified communications channels and ignore the rest. If they remain uncertain, there are avenues that they can turn to verify whether what they have received indeed came from the Government. SNDGG is working with agencies and focusing its initial efforts on SMS and calls, as these are the most widely utilised communications channels. Beyond this, SNDGG will continue to step up efforts to safeguard our systems and applications against evolving cyber threats. For critical systems, SNDGG will strengthen our security monitoring and step up use of sophisticated adversarial pen-testers to make it more costly and difficult for attackers.
Thrust 2: Significantly improve the workplace experience of public officers	
3.	Increase productivity through driving widespread, impactful Artificial Intelligence (AI) adoption

S/N	Initiatives
	Recent developments in AI have enabled its more widespread use, and there is great potential for AI to be more widely adopted in the public sector to drive greater productivity and support Singapore's standing as a leading Digital Government. SNDGG is developing Signature AI use cases to demonstrate the early adoption and impact of AI in public service work, build and anchor capabilities in using the technology, and provide an avenue to scale the use of AI in a strategic area. Examples of use cases being explored by SNDGG to improve productivity include Pair Chat, a ChatGPT-equivalent for public sector use with improved data security; and PQ Assistant, a tool to analyse past Parliamentary Questions (PQs) and help PQ staffers draft replies. Service delivery use cases include tools to help summarise public feedback and compose replies, as well as a recommender for Government support schemes. The list of Signature AI use cases will be continually reviewed and refreshed, as the technology continues to evolve. Beyond developing AI-powered tools, SNDGG will improve WOG access and raise proficiency in the use of AI. SNDGG plans to identity archetypes of public sector work which will most benefit from AI adoption, develop courses and playbooks tailored to these archetypes, and work to integrate these tools into the daily work environment of every public officer (i.e., through their non-S GSIB endpoint device and operational systems).
4.	Redesign the Security Architecture and User Experience for Non-S endpoint devices Currently, our GSIB architecture is secured via a "castle and moat" model, where the network perimeter is primarily security around our on-premises servers, private Cloud, and endpoint devices. As the cybersecurity threat landscape evolves and leveraging Cloud innovation eg. Software-as-a-Service (SaaS) becomes a significant factor to public officer productivity, there is need for a new security paradigm that can better deal with the threat landscape and capture benefits of digital innovations in the Cloud. In the future state, SNDGG will make three shifts to this new security paradigm: a) From network-based to an identity-based security model. There is no "trusted network", and users will authenticate (using biometric token + off-device MFA) for access to each service. b) From "trusted device" to "trusted access" model. Today, GSIBs hold significant amount of data which increases risk of data loss and the number of layers of protection required. Users in future can expect most of their data to reside in and secured in the Cloud. c) From "check once and grant access" to "always checking". Traffic from endpoint and access to service can be continuously monitored and inspected, and service access can be based on specific security posture incorporating time-bound authentication. These shifts allow us to tap on SaaS more confidently to improve officer productivity, while also improving officers' user device experience, with lower start-up time, ability to suspend and resume work instantaneously and better application performance.
Thrust 3: Uplift digital capabilities and competencies to enable deeper and bolder transformation	
5.	Digital competencies for public officers, the ICT&SS workforce and public sector leaders Under DGB1.0, we had set a target of requiring 100% of public officers who require basic digital literacy training to be trained, which supported less digitally-literate officers and established a baseline of digital competencies across Government. To support the next bound

S/N	Initiatives
	of Digital Government, SNDGG and PSD are identifying the next-level basic digital and data competencies that officers should have. However, the key weight of our effort will be on raising the digital and data competencies for (i) “Game-changers” (i.e. Public Service Leaders and key system/ product/ policy-ops owners), and (ii) all Directors and above. This will be critical to driving digital transformation and ensuring policy-ops-tech integration. We will also raise the broad-based capabilities of MX Officers (i.e. MX13 and above) to exploit digital tools and AI to improve their personal and organisational productivity at work. Beyond this, SNDGG will continue to rollout and improve the WOG ICT&SS competency framework to ensure that our WOG ICT&SS workforce is effective and proficient. We will also continue to build the WOG ICT&SS community to allow cross-sharing and keeping up with advancements in technology and good practices across Government.
6.	Forward-deploying GovTech officers to agencies SNDGG is reviewing how to centrally support agencies’ digital transformation beyond uplifting general competencies, in light of increasing manpower constraints and the need for a more sustainable manpower trajectory for the WOG ICT&SS workforce. A model we are exploring is for GovTech to forward deploy capabilities in key areas to support agencies as a general principle. The system modernisation programme (Item 7) is an example of this. Another key area will be to raise product competencies across Government. Digital products are ideally developed through an Agile product development approach – a flexible, iterative and user-centered approach, to maximise our chances of success at solving problems. However, there is a lack of good product development capabilities, including Agile mindsets within Government. SNDGG is therefore developing a digital products incubator programme to provide a structure that supports Agile product development and build a healthy pipeline of innovative and good products. The programme will provide product teams with access to product expertise to help them re-centre the focus on solving problems and start small, build/fail fast, building product capabilities in the process.
7.	Raising capabilities and capacity of local ICT&SS industry Most Government systems and digital products are delivered in partnership with the ICT&SS industry. However, current players lack the required capabilities (e.g. deployment on Cloud, Agile development, data analytics) or the necessary scale to support large ICT&SS projects or forward digitalisation needs. This is evidenced by the challenges from the roll-out of the Human Resource Payroll System. Implementation issues took more than a year to stabilise, requiring an extended Performance Guarantee Period of 15 months. Our earlier plan to develop a National Digital Services Champion is still at a nascent stage. We will need to redouble our efforts to uplift the local ICT&SS sector to better take on Government IT projects, particularly those that are of national interest.
8.	Build up deep AI capabilities to seize opportunities The recent wave of Generative AI has demonstrated the need for Government to level-up its capabilities and keep pace with the speed of innovation in the AI space. Making a concerted effort to develop deep AI capabilities will allow us to take hold of opportunities whenever they arise.

S/N	Initiatives
	To leverage Generative AI, there is a need to develop capabilities, in SNDGG as well as other S&T agencies, to adapt foundational models for enterprise use via fine-tuning or querying internal databases for sectoral/vertical use cases by agencies. There is also a parallel requirement to develop the engineering capabilities to deploy and operationalise these models successfully. This will be achieved through a pipeline of experiments and proof-of-concepts, including but not limited to the Signature AI use cases mentioned in Item 3. Additionally, SNDGG will not have all the answers in this fast-moving AI space. We will need to partner with industry to tap on their expertise and experiences to explore problem statements and enable capability transfer. One example is the AI Trailblazers programme, which is a partnership with Google to accelerate Government AI use cases by providing infrastructure and training support to agencies. In addition, we are also partnering with Stability AI on finetuning their open-source model for local public sector use cases.
Thrust 4: Strengthen enablers for agencies to fully leverage digital technology to enable deeper and bolder transformation	
9.	<u>System Modernisation</u> Today, there are ICT systems in Government which are old, obsolete and/or poorly designed ('legacy'). Proliferation of these systems will cause higher life cycle and modernisation costs, and lower resilience/ performance and agility, affecting agencies' operations and service delivery. We foresee an influx of these systems in the next five years. SNDGG is developing a plan to tackle this at the WOG level. Preliminarily, we have identified some factors that hinder agencies from tackling legacy systems early (e.g. risk of modernising due to the size and architecture of the legacy system, potential need for additional manpower to modernise while the existing systems continue running, and most fundamentally, a lack of capability). As a start, SNDGG will be forming a core group of technical advisors (including potentially supplementing with private sector expertise) and prioritising 2-3 agencies with critical legacy systems. The advisors will work with the agencies to drill deep into technical details and develop a plan to redo architecture. From this process, we will see how to scale the efforts, including extracting key success factors and propagating to more agencies.
10.	<u>Government Data Architecture 2.0 (GDA 2.0)</u> We have enabled quick and secure access to quality data. Under the first Government Data Architecture, we reduced the time taken to share core data to 7 days and established Trusted Centres and Single Sources of Truth to ease access to core datasets and support distribution of clean data. However, we need to do more to facilitate the use of data for operations and service delivery, beyond policy and planning. SNDGG is developing the next phase of the Government Data Architecture (GDA2.0) to (i) achieve seamless discovery of Government data by reducing the time taken from months to days, (ii) optimise cost, performance and security in using data by developing fit-for-purpose common data transfer modalities and (iii) enable trusted monitoring of data access. This includes a WOG Data Discovery platform, streamlined digital data request workflows and tools to support agencies in managing data assets. The goal is to support public officers to more easily discover and tap on data within and across agencies, while allowing agencies to better govern their data assets.

S/N	Initiatives
	Beyond GDA2.0, SNDGG will continue to work with agencies to better leverage and manage their data assets through (i) improving the availability and quality of datasets, (ii) developing and modernising government data systems and architecture to improve utilisation by agencies, (iii) simplifying data policies and regulations and (iv) strengthening data culture and plugging data competency gaps.
11.	Software-as-a-Service Centres of Excellence The shift to Cloud under DGB 1.0 has facilitated greater use of SaaS in the public sector. This provides agencies with a greater choice of best-in-class, ready-to-use solutions, which have fewer administrative overheads compared to traditional enterprise software solutions. However, many agencies currently build systems on SaaS platforms by outsourcing the project to a vendor (traditional turnkey total outsourced), which does not allow agencies to fully reap the benefits of SaaS for system implementation. Hence, SNDGG is developing Centres of Excellence (COEs) for selected SaaS platforms that are widely used by agencies, to build up in-house platform expertise and maximise cost-effectiveness for agencies' selected SaaS platform. The COEs will provide services to agencies such as consultancy and advisory, SaaS implementation for strategic projects, cybersecurity assessment and management, community building and support to develop exit plan/ criteria. SNDGG has identified a few key SaaS platforms and has set up COEs starting with SalesForce and ServiceNow, with more potential COEs based on demand from agencies, quality and technical suitability.
12.	More nimble policies and processes As the ICT&SS Functional Leader (FL), SNDGG will improve our approach to ICT&SS policy and governance to better enable agencies' digital transformation, including improving the capabilities of the policy writers. For example, while the Instruction Manual for ICT&SS ("IM8") has uplifted standards, agencies have also given feedback about the compliance burden imposed by IM8. Criticisms of IM8 include it being one-size-fits-all, overly-prescriptive, leading to downstream admin load (e.g. having to seek waivers, audits) and lagging new developments in tech (e.g. Cloud). SNDGG is exploring how to build greater flexibility into IM8, such as using sandboxes for greater experimentation and an "IM8-lite" so that less sensitive systems need not be subject to the full set of rules. Additionally, with the growing prevalence of AI use cases and AI-powered digital applications, SNDGG is exploring how to balance risk and opportunity in the short term through the iteration of guidelines and standards, with longer term plans to roll out a Public Sector Responsible AI framework and/or technical toolkit to provide practical guidance to assess and mitigate AI-related risks.
Thrust 5: Maximise use of our available resources	
13.	Environmental Sustainability of Government ICT&SS SNDGG is studying how to reduce Government ICT&SS carbon emissions, as part of Government's commitment for the public sector to achieve net-zero emission around 2045. This is a more nascent area of work for SNDGG, and we must find ways to leverage our COG position to drive this. SNDGG is consolidating government data centres, and engaging Cloud service providers on possible inclusion of sustainability criteria as part of bulk tender for Government Cloud.

S/N	**Initiatives**
	SNDGG will work together with MSE to explore how to reduce Government ICT&SS carbon emissions (e.g. green procurement and disposal of Government IT equipment).