FOURTEENTH PARLIAMENT OF SINGAPORE

First Session

REPORT OF THE PUBLIC ACCOUNTS COMMITTEE

Parl. 3 of 2021

Presented to Parliament on

8 February 2021

PUBLIC ACCOUNTS COMMITTEE

Members

Ms Foo Mee Har (Chairman)

Miss Cheryl Chan Wei Ling

Mr Chua Kheng Wee Louis

Mr Derrick Goh

Mr Kwek Hian Chuan Henry

Ms Poh Li San

Mr Saktiandi Supaat

Dr Tan Wu Meng

CONTENTS

Blank Page

REPORT OF THE PUBLIC ACCOUNTS COMMITTEE

Overview

1 The Public Accounts Committee considered the Report of the Auditor-General for the Financial Year 2019/20 and deliberated on the observations in the Report. The Committee also discussed larger issues in relation to financial controls and governance in the public sector, in particular:

a. Risk Management;

b. Government's Response to COVID-19 Pandemic; and

c. Future Risks.

2 The Committee is of the view that it is important for the public sector to have in place an Enterprise Risk Management (ERM) framework at the Whole of Government (WOG) level and at the individual agency level to guide the identification, assessment and management of risks. This would allow the Public Service to innovate while maintaining proper accountability and governance over the use of public funds and resources. The Ministry of Finance (MOF) informed the Committee that it had issued a Finance Circular Minute to public sector agencies in January 2020 covering ERM principles and baseline practices. An ERM Practice Guide was also issued, which covers good practices on ERM governance structure, integration of ERM into strategy planning, ongoing risk management and monitoring, review and revision, and information and reporting. Agencies are required to report the results of their review of ERM practices to MOF and the Accountant-General's Department (AGD). The Committee noted that while many public sector agencies already had their own ERM frameworks before the issuance of the MOF circular minute, the MOF guidance was useful in terms of facilitating a holistic view of risks at the WOG level and ensuring baseline ERM practices across the WOG.

3 The Committee noted that substantial expenditure had been incurred and will be incurred in the fight against the COVID-19 pandemic. New grant schemes were implemented to support businesses and individuals, and to deal with the public health and economic impact of the COVID-19 pandemic. The Committee is of the view that while it is important to respond quickly to the evolving pandemic situation, there is a need to ensure proper controls, governance and accountability over the use of public funds. MOF informed the Committee that it recognises that agencies must continue to maintain proper governance, control and accountability over COVID-19 expenditure, while balancing policy and operational considerations. An inter-agency Budget Implementation Committee (BIC) co-chaired by the Permanent Secretaries from MOF and the Ministry of Social and Family Development was convened in April 2020 to oversee the WOG coordination and timely implementation of COVID-19 support schemes.

4 The Committee also noted that MOF centrally activated Emergency Procurement (EP) procedures at the WOG level for urgent buys by agencies to respond to the COVID-19 crisis in late January 2020, and subsequently centrally deactivated in late August 2020 as the time pressure on procurement had eased off for most agencies. MOF assured the

Committee that the same governance principles apply to EP as with normal procurement, including: (i) the requirement to assess cost reasonableness to the extent possible, taking into account the unique market conditions and time constraints; and (ii) transactions are subject to audit and compliance reviews by relevant authorities. Agencies are required to prepare an Accountability Report to document all EP decisions and the Report must be endorsed by the Permanent Secretary (PS) of the Ministry in person. MOF also issued central guidance and advice to agencies on COVID-19 expenditure and grant programmes.

5 The Committee was concerned about the heightened risks arising from disruptions brought about by the COVID-19 pandemic, in particular risks in the area of public resources and risk from acceleration of digital transformation. The Committee deliberated on two key risk areas: (i) resourcing risks and (ii) new risks and areas of vulnerability arising from an acceleration of Government digital transformation initiatives.

6 On resourcing risks, the Committee asked MOF how it would address such risks, and whether there was a mechanism in place to re-evaluate the need and timeline for large-scale projects as some of the original projections might have changed significantly due to the COVID-19 pandemic. MOF explained to the Committee that the Government had expended significant resources in its COVID-19 response. The Government will face major constraints in its fiscal and manpower position given the weaker economic growth prospects, structural population ageing and international tax pressures. MOF will work closely with agencies to reallocate resources to create space for new priorities and review expenditure for which assumptions may have fundamentally changed, especially for large scale projects such as the Changi Airport Terminal 5 project.

7 On the risks arising from the accelerated pace of digital transformation, the Smart Nation and Digital Government Group (SNDGG) informed the Committee that it had performed external and internal risk scanning, and has identified ten risks based on the WOG Infocomm Technology and Smart Systems (ICT&SS) strategic outcomes. Most of the identified risk domains have been or are being addressed by ongoing efforts. These include strengthening central and agency governance of ICT&SS risks, strengthening agencies' management of data security and cybersecurity risks, and managing human capital risk.

8 The Committee discussed the audit observations in the Report of the Auditor-General.

9 The Committee is of the view that it is important to understand and examine the root causes for the lapses observed by the Auditor-General's Office (AGO) so that appropriate remedial actions can be taken at the WOG level and by the respective public sector agencies. MOF informed the Committee that the respective policy owners in the Government regularly engage agencies to identify the root causes of the systemic audit lapses and put in place measures to help agencies address them and monitor compliance. For example, the root causes of lapses relating to grants management were identified and examined as part of the Grants Management Review. Following the completion of the review, MOF issued a new grants governance framework. MOF had also made use of a number of WOG platforms to communicate common audit findings, root causes and remedial measures to all agencies across different levels of seniority.

10 The Committee also discussed the following two areas highlighted in the Report of the Auditor-General:

a. Weaknesses in Information Technology (IT) controls; and

b. Gaps in management of business grants.

11 The Committee noted that the weaknesses in IT controls included weak controls over the most privileged operating system (OS) user accounts and privileged user activities. There were also weaknesses in terms of the management of third party IT vendors and controls implemented by a private sector partner over its IT system.

12 The Committee noted the efforts taken by SNDGG to strengthen IT governance and enhance IT security at the WOG level, such as adopting technical measures to address IT lapses and taking measures to improve organisational structure and processes. These include: (i) developing a central solution to automate the removal of user accounts no longer required; (ii) strengthening leadership attention on cybersecurity and data issues; and (iii) rewriting the Instruction Manual on ICT Management. SNDGG had also implemented a Third Party Management (TPM) Framework to ensure that the standards of data protection that the Government placed on itself are extended to third parties. This Framework would apply to all third parties engaged by the Government, including IT vendors and all other non-government and private sector partners to whom certain operations are outsourced.

13 On the management of business grants programmes, the Committee noted that MOF had issued a new grants governance framework to all agencies in July 2020. The new framework sets out rules and provides guidance systematically on the entire life-cycle of grants management. The Committee also noted that MOF had set up the Grants Governance Office in October 2019 to coordinate efforts and drive the implementation of the grants governance framework. MOF will ensure that agencies across the different grant sectors reach a baseline level of capabilities by the end of FY 2021.

14 Following the written responses from the ministries, the Committee convened hearings on 17 December 2020 and called upon Permanent Secretaries from MOF and the Ministry of Manpower (MOM) to provide oral clarifications and elaboration of their written responses. The areas discussed at the hearings included risk management, grants governance, accountability and control over COVID-19 expenditure and grants, as well as future risks pertaining to management control and financial expenditure.

15 The Committee would like to emphasise the following points:

a. The Committee welcomes the actions taken to raise ERM capabilities across the public sector and calls upon MOF and the public sector agencies to give urgent attention towards levelling capabilities to ensure continued progress in the development and implementation of ERM. To fully reap the benefits of ERM, it is important for ERM practices to be implemented in a consistent manner on the ground and to ensure that new and emerging risks in the operating environment are captured and adequately addressed. Having an ERM framework in place will allow the public sector to be cognisant of trade-offs between controls and flexibility, and enable the public sector to

innovate and become more nimble in addressing existing and future risks while maintaining proper accountability and governance over public resources.

b. Given the COVID-19 pandemic situation, the Committee agreed that there was a need for the Government to act swiftly. Where Emergency Procurement was needed, the Committee noted that Government agencies were still required to conduct proper evaluation before award and proposals were assessed based on the published evaluation criteria. In addition, agencies were required to assess cost reasonableness to the extent possible for EP, taking into account the unique market conditions and time constraints. This allows a balance between swift action and having adequate checks and balances. The Committee noted that MOF is taking a multi-pronged approach to improve the Government's resilience in managing emergency situations whilst balancing the need for fiscal prudence and accountability. Key COVID-19 expenditure would be subject to ex-post analytics and audit checks. Agencies which used EP procedures should maintain accountability over the use of public funds, including the timely submission of Accountability Reports.

c. The Committee noted the cross-agency collaboration and efforts in administering COVID-19 related grant schemes. The Committee noted that the BIC provides guidance to agencies to ensure that COVID-19 measures are reaching targeted groups from a citizen- and enterprise-centric perspective. Going forward, it is important for agencies to consider possible scenarios when allocating their resources and be nimble in responding to fast-evolving situations. Agencies should continue to consider the needs of various segments of the population especially the vulnerable groups, such as low-wage workers and self-employed persons who have been significantly affected by the pandemic.

d. Drawing lessons from the pandemic, the Committee is of the view that data and technology would be key enablers for agencies to better plan and collaborate together and deliver programmes more effectively. Given the higher incidence of cyber attacks globally, IT controls must remain robust and adequately address IT-related risks, such as cybersecurity and data security risks. The Committee noted that while automation is central to SNDGG's approach to addressing IT lapses, automation alone is not enough. Technical solutions would also require human supervision, changes in processes and adherence to them.

e. On the lapses and weaknesses observed in the Report of the Auditor-General, it is important for agencies to examine and investigate the root causes for the lapses so that appropriate remedial actions can be taken at the WOG level and by the respective public sector agencies.

16 The Committee's enquiries and the agencies' responses, as well as MOF's and SNDGG's responses on measures at the WOG level, are discussed in the following sections.

Committee's Enquiries and Ministries' Responses

A. Observations in the Report of the Auditor-General for the Financial Year 2019/20

Root Cause Assessment on Audit Observations

17 The Committee deliberated on the audit observations on weaknesses in IT controls at the Ngee Ann Polytechnic (NP) and Republic Polytechnic (RP), lapses in procurement and contract management at the National Library Board (NLB), and gaps in management of business grant programmes at the Workforce Singapore Agency (WSG) and Enterprise Singapore Board (ESG).

18 The Committee asked MOF on the framework in place at the WOG level and within the respective agencies to assess and examine the root causes of the lapses identified, and to ensure that remedial measures taken will fully address root causes. The Committee also asked the Ministry of Communications and Information (MCI) and Ministry of Education (MOE) on whether an assessment was performed to ascertain the root causes of the lapses and the results of the assessment.

Ministry of Finance

19 On the assessment and examination of root causes of the lapses identified by AGO, MOF explained that the respective policy owners regularly engage agencies to identify the root causes of systemic audit lapses and put in place measures to help agencies address them and monitor compliance. For example, the Government Procurement Function Office in MOF is working with the Building and Construction Authority to simplify rules, improve guidance given to officers and raise capabilities to address the root causes of recurring lapses in construction procurement and contract management. For grants management, the root causes of the lapses were identified and examined as part of the Grants Management Review that was completed in 2019. The implementation of the recommended remedial measures arising from the Review will be overseen by an inter-agency committee.

20 There are also WOG platforms to communicate common audit findings, root causes, and remedial measures to all agencies across different levels of seniority. These platforms include: (i) the Deputy Secretaries/Chief Executives and Heads of Organs of State dialogue on audit matters with the Auditor-General and the Accountant-General; (ii) Finance Leaders Meeting; (iii) Internal Audit Round Table involving Internal Audit leaders across WOG; and (iv) Sharing and dialogue sessions between each Ministry family and AGO, MOF, and AGD.

Ministry of Communications and Information

21 MCI informed the Committee that NLB had convened an internal review panel reporting to the CEO and the NLB Board to identify the contributory factors to the lapses and recommend remedial actions to mitigate the risks of recurrence. The panel assessed that the lapses were primarily due to weakness in duty of care on the part of NLB officers

involved in the procurement and project management aspects. The panel's recommendations have been endorsed by both the Board and the Board-level Audit and Risk Committee. Following the panel's report, disciplinary actions have been taken against officers found to be negligent in discharging their duties.

22 To further strengthen officers' understanding of their procurement roles, NLB had stepped up briefings and enhanced guidance on the roles and responsibilities of officers involved in each stage of the procurement cycle. This is on top of detailed checklists covering each stage of the procurement cycle. Since April 2019, NLB had reinforced the clarity of the workflow on approving authority matrix for In-Principle Approval (IPA) of variation works and the Contract Variation execution workflows enhanced to tighten approval and tracking of such works. NLB will conduct regular sharing sessions to remind its Project Managers of the tightened IPA Standard Operating Procedures. NLB will also explore automating online tracking of variation orders for development projects and hence project cost utilisation, with system roll-out targeted in FY 2021.

Ministry of Education

23 MOE informed the Committee that for NP, the privileged database account activities selected for review were not formally discussed and approved. For its NPal IT system, only 6 out of the 38 actions that could be performed by the privileged database user accounts were picked out for review. NP assessed that the process for selecting these 6 actions could have been more thorough, and the inadequacy of the selection would have been flagged if the proposed selection supported with proper risk assessment was tabled for formal discussion and approval by its ICT and Digitalisation Steering Committee (IDSC). NP had since strengthened its risk assessment approach which was validated by its auditor. Since March 2020, NP had monitored 32 out of 38 actions, with the 6 remaining actions assessed to be of lower impact to IT security. To strengthen existing practices, NP had engaged a consultant to conduct a more comprehensive risk assessment for all its systems. The review is targeted to complete by Q1 FY 2021 and recommendations would be tabled at its IDSC for approval.

24 In the case of RP, MOE informed the Committee that at the point of implementation of the system interface with the appointed bank in 2011, the file encryption capability for the electronic payment batch files was not yet available. When the encryption feature was subsequently made available by the bank, RP did not in its periodic reviews re-evaluate and adopt the additional security controls. The encryption feature would have reduced the risk of unauthorised changes to the payment files significantly. RP had since encrypted its payment batch files and ensured that encryption is used in other similar financial systems. RP would also carry out periodic checks on external systems that it interfaces with, to identify additional enhancements and controls that can be implemented to further reduce their risks.

Observations on Grants Management

25 The Committee noted the audit observations from the thematic audit on business grant programmes managed by WSG and ESG. The Committee noted that the two agencies had put in place policies and procedures to manage the selected grant

programmes. However, the area of grants monitoring and review could be further strengthened, particularly where the administration of the grant programmes had been outsourced to external Programme Partners (PPs).

26 The Committee is of the view that while it is important to process and disburse grants in a timely manner to benefit recipients, there is also a need to ensure proper accountability for the public funds used. In this regard, the Committee had asked MOM and the Ministry of Trade and Industry (MTI) on whether there are measures implemented or to be implemented (including implementation timeline) to ensure that:

a. There is adequate oversight over the PPs and that PPs are competent and are adequately equipped to manage and administer grants; and

b. The need for speed in grant processing and disbursements is balanced with proper controls and governance.

27 The Committee also asked MOF on whether there are measures implemented or to be implemented at the WOG level to ensure that:

a. The capability of public sector agencies in managing grant programmes is raised to a higher level;

b. There is adequate oversight and consistent practices across PPs and that PPs are competent and adequately equipped to manage and administer grants;

c. The key performance indicators (KPIs) stipulated in grant agreements are regularly updated to ensure that they remain relevant and there is monitoring of the KPIs to ensure that any gaps in performance are followed up on a timely basis;

d. The need for expeditious grant disbursements is balanced with proper controls and governance; and

e. The effectiveness of grant schemes administered by various agencies is assessed to determine if the grant schemes have achieved the desired outcomes.

Ministry of Manpower

28 MOM informed the Committee that while MOM and WSG had put in place proper controls and guidelines to manage the grant programmes prudently and to prevent fraud, they acknowledged AGO's observations that there were areas for improvement. Where there were operational reasons to provide flexibility to the PPs to account for the specific circumstances of their client base, these should be properly scoped and defined. Baseline requirements should also be maintained across all PPs. MOM and WSG were firmly committed to ensure the good governance and effectiveness of its programmes and the prudent use of public funds.

29 MOM added that WSG currently works with about 30 Professional Conversion Programme Partners (PCP PPs) to run close to 100 Professional Conversion Programmes

(PCP) in about 30 sectors. WSG evaluates the entities prior to appointing them as PCP PPs. WSG assesses the entity's ability to engage and reach out to employers for the PCP, as well as its past track record (placements and compliance) in administering programmes. To ensure that PPs are adequately resourced, WSG also funds the PPs' administrative costs.

30 WSG would strengthen the supervisory controls and administration processes over the PPs. To ensure consistency of practices across PPs, WSG had developed a new PCP PP guide in December 2020 which sets out baseline requirements for compliance from 2021 onwards. PPs would be required to comply with all guidelines in this new guide. Meanwhile, WSG had reiterated to all PPs the need to adhere to the PCP administration process. In particular, the importance of ascertaining that participants will meet the criteria for career conversion was emphasised, as well as close tracking and timely reporting of key programme outcome indicators. Starting from 2021, WSG would conduct regular sampling checks on the PPs. WSG would also enhance its digital systems from Q1 2021 to better administer PCP applications to reduce processing errors and better mitigate the risk of fraud and abuse.

31 WSG would engage PPs more regularly at the senior leadership level to emphasise the importance of good governance in grant administration from Q1 2021. For new PPs, WSG would also put in place a more thorough onboarding process to underscore the importance of fulfilling their administrative responsibilities and training their staff to perform these functions in accordance to the new PP guide in Q1 2021. WSG would closely monitor the effectiveness of these enhanced measures and implement additional controls to ensure adequate oversight of the PPs where necessary.

32 The Committee also asked MOM (i) how it monitors the outcomes of its grant programmes to ensure their effectiveness; and (ii) whether and how MOM conducts performance evaluation to assess the effectiveness of its various grant programmes, specifically the PCP.

33 MOM informed the Committee that MOM and WSG conduct regular reviews of grant programmes to determine their effectiveness in meeting programme outcomes, and to identify areas of improvement. There are periodic updates to MOM's and WSG's Management on indicators such as the take-up rate and profile of grant beneficiaries to assess if PCPs help jobseekers make successful career transitions. Attention is paid to the outcomes for the more vulnerable mature workers and the long-term unemployed.

34 On AGO's observation that three of WSG's PPs did not carry out adequate verification of career conversion involving 15 PCP participants, MOM said that WSG has since reviewed each case and verified that all 15 participants had changed their job scopes and successfully converted into new job roles through their respective PCPs.

35 As for AGO's observation that there was inadequate monitoring of programme outcomes for 10 out of 16 PCPs checked, MOM explained that the PPs did not collect the complete set of performance indicators required by WSG, and had varying practices in collecting the information. WSG has since reviewed and streamlined its approach. Henceforth, PPs would focus on reporting the two most important outcome indicators which directly measure how PCPs help jobseekers to reskill and transit into new jobs.

36 Beyond the cases checked by AGO, WSG initiated additional checks of all PCP placements since 2016 to ensure that the lapses were not systemic. The review of over 15,000 cases was completed in December 2020 and WSG had identified 80 cases for further checks.

37 WSG had also reiterated to all PPs the importance of adhering to the PCP administration process, including the proper assessment of career conversion for participants, as well as the importance of close tracking and timely reporting of key programme outcome indicators. To ensure compliance with these requirements, WSG would conduct sampling checks of PCP placements by its PPs on a regular basis.

Ministry of Trade and Industry

38 MTI informed the Committee that ESG has continuous and close interactions with its PPs, such as the Trade Associations and Chambers (TACs), which go beyond the administration of grant schemes. ESG's experience with the TACs allows it to understand their directions, capabilities, and challenges, which informs ESG's assessment of the TACs' ability to be effective PPs. Before appointing TACs as PPs, ESG will assess the track record of the TACs to ensure that they have the capabilities to deliver on the projects. Given their industry experience and knowledge of the small and medium-sized enterprises, the appointed TACs are well-placed to handle the projects. Following their appointment as PPs, ESG continuously engages the TACs to ensure adequate oversight from start to end.

39 For every project administered through a PP (i.e. TAC), ESG will issue a Letter of Offer to the TAC stating the conditions of the grant, including the contractual responsibilities and reporting requirements of the TAC. TACs must comply strictly with these terms and conditions.

40 Before making disbursements to a PP, ESG will verify that the project deliverables have been met. All incurred expenses are also subject to audit checks by ESG's independent auditors. As an additional safeguard, ESG has appointed auditors to conduct post-disbursement checks on PPs. ESG has also implemented enhanced, risk-based safeguards to ensure accountability for Government funds disbursed to PPs since February 2020, such as requiring PPs that receive cash advancements to set up a separate bank account or cost centre.

41 On the issues noted in AGO's observations, MTI informed the Committee that ESG had since completed a review of (i) its policy on manpower support for TACs and (ii) its controls and governance over grant disbursements made by TACs to participating companies. Changes to manpower support will be implemented with effect from July 2021. On grant disbursements, ESG had further strengthened its checks to ensure TACs' compliance to grant conditions.

Ministry of Finance

42 On grants management, MOF informed the Committee that, following the completion of the Grants Management Review in 2019, MOF had issued a new grants

governance framework to all agencies in July 2020. The new framework sets out clear rules and provides guidance on the entire grants management process – from grant design, approval and disbursement, to monitoring and anomaly detection. It also emphasises the importance of proper planning and risk management, to ensure effective use of public funds and to safeguard against fraud and abuse. The rules are also supplemented by a good practice guide that provides helpful examples and practical advice for all agencies.

43 MOF set up the Grants Governance Office in October 2019 to coordinate efforts and drive the implementation of the new grants governance framework to ensure proper financial governance and strengthen capabilities in grants administration. It supports the Grants Management Committee (GMC), which brings public sector agencies together to coordinate information sharing, harmonise processes and develop system solutions to improve grants management. The GMC has also drawn up capability-building roadmaps, which outline a multi-year plan to deepen the agencies' capabilities in system and data analytics, fraud detection and investigation to guard against lapses, fraud and abuse. MOF aims to ensure that agencies across the different grant sectors reach a baseline level of capabilities in these areas by the end of FY 2021.

44 Apart from raising capabilities of agencies in grants management, MOF recognises that PPs also play an important role in the administration of grant programmes. Hence, MOF has incorporated principles and rules on the management and monitoring of intermediaries such as PPs into the grants governance framework for agencies' compliance. In particular, agencies are required to establish and document clear roles and responsibilities with the intermediaries, and a governance framework to manage and monitor them. Sampling checks are recommended to ensure that the intermediaries duly discharge their responsibilities.

45 The grants governance framework requires agencies to include grant deliverables, KPIs and other performance measures (where applicable) in their grant agreements. In addition, agencies should consider reviewing their grant schemes every three to five years, or when priorities change. Accordingly, agencies should update the performance measures during the review where appropriate. Agencies are also required to track performance measures and document the monitoring of project performance.

46 On controls over grant disbursement, MOF informed the Committee that agencies are required to put in place processes and guidelines to ensure that grants are disbursed according to the agreed quantum, milestones and criteria. These include proper checks and approval of grant claims, as well as segregation of roles for processing and approving disbursements. Agencies are also required to put in place measures to recover disbursed grants in a timely manner, if they are misused or erroneously disbursed. MOF added that the need for expeditious grant disbursements should not compromise proper controls and governance. Under the new grants governance framework, agencies will have to first consider the policy intent of the grants and risks involved, before putting in place appropriate safeguards to actively manage the risks of fraud and abuse.

47 As regards the assessment of grant scheme effectiveness, MOF informed the Committee that agencies are required to evaluate whether their grant schemes are achieving the intended objectives. In addition to agencies' reviews, MOF conducts reviews on government programmes and grant schemes administered by various agencies.

Key learning points from these reviews are shared widely across the public sector through learning sessions, forums and online circulation.

Observations on IT Weaknesses

48 For IT-related lapses, the Committee noted that there were weaknesses in IT controls across several public agencies, including weak controls over the most privileged user accounts and inadequate reviews of activities carried out using privileged user accounts. The Committee also noted that controls over third party vendors and partners could be strengthened. The Committee noted that SNDGG has put in much effort to strengthen IT governance and enhance IT security at the WOG level. Given the increasing pace of digitalisation and outsourcing of IT operations in the public sector, IT-related risks such as data security and cybersecurity risks will remain as key risks for the Government. In this regard, the Committee asked SNDGG for an update on the following remedial actions and measures that were previously communicated to the Committee in October 2019:

a. Details of measures that have been taken or will be taken (including implementation timeline) to ensure that the most privileged OS user accounts are used by authorised users appropriately and that there is monitoring and review of activities using the privileged accounts;

b. Details of measures that have been taken or will be taken (including implementation timeline) to ensure that the scope and responsibilities of IT vendors are properly defined and how such vendors are being managed; and

c. Any new developments since then.

49 SNDGG informed the Committee that while automation is central to SNDGG's approach to addressing IT lapses, automation alone is not enough. Technical solutions would also require human supervision, changes in processes and adherence to them. There is a need for a change in culture and raise the awareness and knowledge of public officers towards cyber and data security to complement these technical solutions.

a. Technical Measures

50 SNDGG informed the Committee that it is on track to introducing tools to automate tasks and address the IT lapses.

51 (i) Management of account and user access rights: Since October 2019, SNDGG had implemented a solution for 38 agencies that would alert agencies to staff movement and role changes, so that agencies could manually remove user accounts that were no longer required. However, this solution still requires a manual check, and SNDGG would develop a central solution to include the automation of the removal process to reduce room for human error. SNDGG targeted to complete building this central solution by December 2021, after which SNDGG and agencies would integrate all systems with the central solution over the following three years. SNDGG was on track to implement this for high-priority systems by December 2023 and the remaining systems by December 2024.

52 (ii) Review of privileged users' activities: SNDGG was on-track to implement this for high-priority systems by December 2022. Since April 2020, SNDGG had completed a pilot involving 15 agencies. SNDGG was refining the imputed detection rules to monitor the different types of logs including operating systems, databases, networks, applications and security, and logic to improve the detection efficiency, and would progressively scale this up to all agencies starting from January 2021.

b. Measures to Improve Organisational Structure and Processes

53 SNDGG had also taken steps to strengthen organisational structures and processes for greater ownership to ensure that lapses were addressed, lessons were learnt, and improvements were continuously made.

54 (i) Strengthened leadership attention on cybersecurity and data issues: The Agency Chief Security Officer and Chief Data Officer are required to report key cybersecurity and data issues directly to the Head of Agency. SNDGG had also tabled the WOG Governance report at a senior-level forum.

55 (ii) Updated ICT policies: The rewritten Government Instruction Manual 8 (IM8) had been progressively published from Q3 2020. The rewritten IM8 spells out the policies and the intent; the standards required to meet the policy intent; and the guidelines that may be adopted to meet such intent. The emphasis on outcomes ensured that system owners take responsibility of their systems and do not mechanically follow instructions. The implementation of the rewritten IM8 was also accompanied by change management efforts including briefings to all agencies. Role-based training for IT management was also being developed and would be available from January 2021.

56 (iii) Strengthening the audit process: A WOG Governance system would utilise audit and incident data to predict potential governance risks to IT systems. Pilot agencies would come onboard in Q1 2021, with roll-out targeted in Q2 2021.

c. Raising Awareness of ICT Governance

57 SNDGO had implemented the mandatory cybersecurity awareness programme for all public officers to raise the awareness of officers on cybersecurity threats. All public officers had completed the programme for 2019, and the programme had been updated in 2020 to include both cyber and data security. Officers are required to complete the assessment by 31 December annually.

d. Measures to Improve the Management of Vendors

58 In April 2020, the Government implemented a Third Party Management (TPM) Framework to ensure that the high standards of data protection that the Government placed on itself are extended to third parties. This TPM Framework applies to all third parties engaged by the Government, including IT vendors and all other non-government and private sector partners to whom certain operations are outsourced. The TPM Framework included (a) standardised contract templates to better inform Government vendors of what is expected of them, and how to interact with agencies that engage them; and (b) guidance to agencies on managing and monitoring their vendors' performance

throughout the project life cycle and auditing their vendors' compliance with stated policies.

Public Sector Data Security

59 SNDGG informed the Committee that it has strengthened the public sector data security regime in the following ways:

a. Sharper audit focus and stronger TPM processes;

b. Timelier detection of and enhanced management of data incidents;

c. Strengthened data security accountability across all groups of public officers;

d. Instituted a clearer and more structured approach to build a data security-conscious culture within the Public Service;

e. Strengthened organisational structures to drive and manage data security; and

f. Improved transparency of the public sector data security regime.

Enhancing Data Policy, Processes and Capability

60 SNDGG informed the Committee that the Government had made progress in implementing technical and process measures to strengthen public sector data security. In October 2019, 4 baseline technical and process measures were implemented across the Public Service. The remaining technical measures were on-track to be implemented as planned; 80% of the systems would be covered by the end of 2021 and all systems by the end of 2023. These measures include tools that (a) prevent the loss of sensitive data across all government systems and devices; and (b) automate user account management to ensure regular and timely reviews of access to IT systems containing sensitive data.

61 The Committee noted that new processes had also been implemented to ensure a more coordinated and effective response to data incidents across the WOG. The Government Data Security Contact Centre (GDSCC) was set up in April 2020 for members of the public to report data incidents involving public agencies. This augmented the Government's ability to detect and respond to data incidents for swift remediation efforts. Starting from March 2021, all public agencies are required to carry out cyber and data security incident exercises annually, to ensure that they are well-prepared to detect and respond to cyber and data incidents.

62 SNDGG also informed the Committee that it had embarked on a campaign to build a culture of excellence in "Using Data Securely" within the public service, so that public officers move beyond mere compliance with baseline requirements to proactively identifying and managing data security risks. In addition, SNDGG had identified data security competencies and training programmes required for public officers to perform their roles well.

Strengthening Organisational Structures, Transparency, and Accountability

63 The Committee noted that the Government had introduced and strengthened organisational structures to drive a resilient public sector data security regime that could

keep up with emerging threats and new technologies. The Digital Government Executive Committee for Cyber and Data, chaired by the PS (SNDGG), had been established as the high-level body to oversee public sector data security and cybersecurity. The Government Data Security Unit was also set up within SNDGG to drive and coordinate data security efforts across the public sector.

64 SNDGG informed the Committee that the Government had also developed a TPM Framework for third parties such as vendors and contractors that handle Government data on behalf of the Government, to establish high standards of data protection on these third parties.

65 In addition, amendments to the Personal Data Protection Act (PDPA) were passed in Parliament on 2 November 2020, to hold third parties and non-public officers accountable for recklessly or intentionally mishandling personal data. This would align the PDPA with the Public Sector (Governance) Act in terms of individual accountability and penalties for the egregious mishandling of personal data.

66 SNDGG also informed the Committee that it had launched a new microsite to provide the public with information on the Government's approach to public sector data security. The microsite contains the Government's personal data protection policies, third party management policies and the GDSCC incident-reporting platform. On 11 November 2020, SNDGG published the inaugural *Annual Update on the Government's Personal Data Protection Efforts* that highlighted the initiatives undertaken by the Government to safeguard personal data. Going forward, the *Annual Update* will be published on the microsite every July.

Third Party Management

67 Non-government and private sector entities to whom operations are outsourced fall under the broad category of third parties which are bound by the TPM Framework set out earlier. Amendments to the PDPA have also been made, to hold third parties and non-public officers accountable for certain mishandling of personal data. The guidance on security requirements would ensure that the vendors are contractually obliged to comply with the security requirements that will address the weakness, and that they will be audited on a regular basis depending on the risks of the system.

Data Incidents

68 The Government had strengthened oversight and raised awareness of cyber and data security amongst public officers. There was a heightened level of vigilance among public officers. Data incidents were also detected and managed more effectively. There were fewer data incidents reported in FY 2019 as compared to FY 2018, due to an improved awareness and understanding among officers of what would constitute a data incident and to report all incidents, no matter how small, so that the rest of the Public Service can learn from them. Lessons from such data incidents are also shared widely, through newsletters, advisories and publications, within the WOG. In addition, SNDGG will be implementing a WOG Data Loss Prevention programme to prevent unintentional disclosure of data.

69 SNDGG expects the full effects of its initiatives to address cybersecurity and data security risks to only be visible in the next two to three years, when the initiatives are implemented more widely and have more traction.

B. Risk Management

70 The Committee is of the view that an Enterprise Risk Management (ERM) framework is important as it could guide risk identification, assessment and management in public sector agencies. The Committee asked MOF on its role in advising public sector agencies on developing and implementing risk management frameworks. The Committee also asked MOF whether there is a WOG ERM framework in place and whether each public sector agency also has its own ERM framework.

71 In addition to questions on ERM frameworks at the WOG level, the Committee also asked MCI, MOE and MTI whether there is a risk management framework in place within their respective Ministry family and at the individual statutory board level.

Ministry of Finance

72 MOF informed the Committee that it adopts a holistic approach across public sector agencies to strengthen risk management and culture. MOF is part of a central WOG Risk Management team that sets common standards for ERM practices across public sector agencies, and appoints the relevant functional leaders to build capabilities in managing risks in functions that exist in all agencies, like Finance, Human Resource, Procurement and Information Technology. Functional leaders report to Head Civil Service, PS (Finance) and a few other Permanent Secretaries overseeing key domain areas like human resource and IT regularly, and are responsible for (i) identifying risks and risk owners; (ii) ensuring that systems for managing risks are in place; (iii) building capabilities; (iv) setting standards; and (v) monitoring compliance of risk measures.

73 MOF informed the Committee that agencies across the WOG face and manage a wide, heterogeneous portfolio of risks. At the agency level, each agency is required to tailor its risk management approach according to its business context, and to integrate risk management into its policy planning and day-to-day operations. To strengthen risk management, MOF and the AGD issued a Finance Circular Minute in January 2020, on the *Introduction of Enterprise Risk Management Principles and Baseline Practices for the Singapore Public Service*. An ERM Practice Guide, setting out key ERM principles and practices, was also issued for public sector agencies' reference to customise practices that would suit their context and needs.

74 Together with the Finance Circular Minute and ERM Practice Guide, a self-assessment checklist was also issued to help agencies review their ERM practices and assess their ability to respond to existing and emerging risks. Agencies were required to submit their returns to MOF and AGD. As of June 2020, all agencies had started or planned to implement the required ERM practices, where they had not been in place. About 20% of agencies had fully implemented all the baseline ERM practices, 60% of agencies were progressing well and will fully implement the baseline requirements soon, and the remaining agencies would implement the baseline requirements in the near future. Reviews of agencies' practices will be conducted at regular intervals with the next review in 2022. The WOG Risk Management team will work with agencies to ensure they have met the ERM standards. To further incentivise agencies to level up their ERM capabilities and put in place the appropriate ERM structures and processes, an overview of agencies'

returns and how they compare with other agencies, including detailed results within each Ministry Family, were circulated to all agencies.

75 To support Public Sector Leaders in setting the proper leadership tone, the WOG Risk Management team developed a Communications Kit to agencies on WOG Risk Management in September 2020. This kit outlined the need to strengthen risk management across the Public Service, highlighted key systemic and operational risks, and updated agencies on the centralised support available. The WOG Risk Management team will also continue to strengthen agencies' and officers' ERM capabilities, such as through facilitating the exchange of good practices and learning points amongst agencies.

76 MOF is mindful that risk management has to be contextualised to the operating environment and evolving scenarios faced by each agency. Therefore, MOF has given agencies and their ERM committees operational flexibility in the ERM implementation. For example, the baseline practice for every agency to maintain an agency-wide consolidated risk register does not dictate the exact risk parameters and risk matrix to use, thus enabling agencies to tailor their risk register to suit their operational needs.

Ministry of Communications and Information

77 MCI informed the Committee that its ERM focused on managing risks across the entire Ministry and involved strategic risk, financial risk, operational risk, and compliance risk. MCI's ERM framework comprised environment scanning, risk assessment and risk treatment. As part of the framework, MCI would identify and analyse risks by looking at factors and causes for the risk event, while putting in place controls for threats identified and establishing recovery procedures for the potential consequences.

78 The MCI family implemented the ERM Framework at the Ministry and statutory boards individually to identify and assess risks, define action plans to mitigate risks and continually monitor and evaluate the effectiveness of these plans. MCI's Risk Committee, chaired by the PS, would provide guidance and direction for the implementation of the ERM framework in MCI. Its Risk Management Office, led by the Chief Risk Officer, would coordinate and monitor the overall risk strategy and facilitate key risk activities. The Ministry-level risk register comprising divisional level risk registers was overseen by divisional directors and maintained by the individual divisions. Its risk register is reviewed annually as part of workplan reviews and presented to PS.

79 MCI also explained how risk management is carried out in its statutory boards. For example, at NLB, each risk area is owned by a specific member of the senior management team. On a half-yearly basis, a review of the enterprise risks is conducted and reported to the NLB Board through the Board-level Audit and Risk Committee (ARC).

80 MCI's risk culture is shaped from top-down and bottom-up. While the Risk Committee chaired by the PS would shape the overall direction, divisions would also incorporate risk assessment as part of their annual workplans to support the overall MCI priorities. In addition, there is regular knowledge exchange between MCI and its statutory boards to raise awareness of best practices that strengthen governance. To put in place a proactive culture of risk management, divisions identify new risks as a result of their evolving work and priorities. This is annually taken stock at the workplan discussions.

Ministry of Education

81 MOE informed the Committee that it had put in place an ERM Framework to manage all risks holistically. ERM is overseen by a committee chaired by MOE's PS and comprised all members of the senior management team. MOE organised its ERM by risk clusters and every risk in the risk clusters has an assigned risk owner. The risk owner would closely monitor and review the management of the risk. The risk owner also has to look at the risk management not just from his/her Division's perspective, but is also expected to work with other relevant divisions and agencies to obtain data and put in place a holistic set of mitigation measures.

82 MOE has an annual ERM review and assessment cycle which involves reviewing and assessing all risks, and identifying emerging risks in response to new scenarios from environmental scans or newly-discovered "blindspots" based on insights from past incidents. Key risk findings are then incorporated into the development of divisional strategies and annual workplans.

83 In driving a risk-aware culture, MOE has put in place communication channels to inform staff at multiple levels within MOE HQ – general staff are informed of risk matters via various risk owner-initiated channels on matters such as IT security, workplace safety and staff professional conduct.

84 MOE statutory boards are subject to prevailing WOG ERM Framework and are expected to comply with the baseline standards and requirements. There is an oversight body in each statutory board, normally chaired by a Board Director, which is responsible for ERM policies and procedures. Each oversight body meets at least once a year and there are practices in place to ensure regular review of risks. Having their own oversight bodies allows agencies the flexibility to assess their respective risk posture and appetite and be able to respond quickly to change and new risks. To address any identified gaps from the self-assessments conducted in April 2020, they have conducted reviews and are in the midst of implementing the necessary enhancements to ERM in their respective organisations.

Ministry of Trade and Industry

85 MTI informed the Committee that each MTI statutory board generally has ERM frameworks and processes that are approved by each statutory board's Governing Board, to identify and monitor risks specific to their mandate, develop risk treatment plans, and periodically update risk registers. Each statutory board also has either a Risk Committee or an ERM Steering Committee (comprising senior management members), which prioritises key risks and implements risk mitigation plans. A central team (such as an ERM secretariat) coordinates efforts to examine risks and risk mitigation controls in each statutory board, and maintains the risk register where key changes are endorsed by the Risk Committee or ERM Steering Committee.

86 MTI officers work closely with statutory boards to surface key risks to MTI's senior management. MTI officers from the relevant policy desks are typically present at

the meetings of statutory boards' Governing Boards, and this provides access to information on how statutory boards are managing their risks. These officers will escalate any risks for attention as necessary.

87 In addition, MTI statutory boards are required to complete a self-assessment checklist each year to validate their compliance with the key principles embodied in the MTI Code of Corporate Governance for Statutory Boards. This Code includes areas such as Board matters (e.g. appointment, composition, independence), conduct of Board affairs, audit and accountability (including the establishment of an Audit Committee, internal controls, and internal audit functions). Besides the Code, the statutory boards are also required to annually declare their compliance with their respective statutory boards' Act and Government Instruction Manuals. The statutory boards are required to provide explanations for any deviation and the results are tabled and discussed at the MTI Audit Committee Meeting. The policy divisions overseeing each statutory board will also review the results to see if improvements are required.

88 Risk management at MTI-HQ is overseen by senior management. MTI-HQ will further strengthen its risk management capabilities by expanding the current remit of the Audit Committee, co-chaired by PS (Trade and Industry) and PS (Development), into an Audit and Risk Committee, which will oversee enterprise risk at MTI-HQ.

C. Government's Response to COVID-19 Pandemic

89 The Committee noted that substantial expenditure would be incurred in the fight against the COVID-19 pandemic. New grant programmes had been implemented by the Government to support businesses and individuals, to deal with the public health and economic impact of the COVID-19 pandemic. Apart from grant programmes, there were other new areas of Government spending such as the establishment of community isolation and quarantine facilities.

90 The Committee asked MOF, MOM and MTI on how they maintain oversight and ensure adequate governance and controls over the large COVID-19 expenditure, and how agencies maintain a balance between speed of response and the need for accountability and prudence in spending public funds.

Ministry of Finance

91 MOF informed the Committee that it recognises that agencies must continue to maintain proper governance, control and accountability over COVID-19 expenditure, while balancing policy and operational considerations in this unprecedented time. An inter-agency Budget Implementation Committee (BIC) co-chaired by the Permanent Secretaries from MOF and the Ministry of Social and Family Development was set up in April 2020 to oversee the WOG coordination and timely implementation of the Budget COVID-19 support schemes. The BIC provides guidance to agencies to ensure that COVID-19 measures are reaching targeted groups from a citizen- and enterprise-centric perspective. MOF supports the BIC's work to monitor the governance of key COVID-19 schemes, calibrate controls based on the risk of abuse, and balance between convenience and control.

92 Building on the work of the BIC, MOF will also work with agencies to evaluate the outcomes and effectiveness of key COVID-19 schemes, when more data is available. Key schemes include the Jobs Support Scheme, Self-employed Persons Income Relief Scheme, and COVID-19 Support Grant. These reviews will be reported to various forums, including the BIC.

93 For procurement, current rules allow for Emergency Procurement (EP) procedures to be undertaken for urgent buys to respond to situations such as the COVID-19 crisis. EP procedures enable faster procurement to meet and respond to operational needs in an emergency. Compared to normal procurement, the EP procedures allow for shorter tender and quotation opening periods, higher procurement limits for small value purchases and quotations, as well as expedited approval process. The same governance principles and controls apply to EP as compared to normal procurement to ensure that expenditure incurred under EP is properly managed and accounted for. Government agencies are still required to conduct proper evaluation before award and proposals are assessed based on the published evaluation criteria. In addition, agencies are required to assess cost reasonableness to the extent possible for EP, taking into account the unique market conditions and time constraints.

94 Activation and deactivation of EP at the agency level is approved by the PS of the Ministry. During the COVID-19 crisis, MOF centrally activated EP at the WOG level in late January 2020 to enable agencies to use EP procedures to buy more quickly and more flexibly to respond to the crisis, as it was a situation impacting public health and safety on a national scale. MOF centrally deactivated EP in late August 2020 as the time pressure on procurement of COVID-19-related supplies and services had eased off for most agencies.

95 As with all procurement, transactions done during this period are also subject to audit and compliance reviews by relevant authorities. Agencies must also prepare an Accountability Report to document all EP decisions. The Accountability Report must be submitted to and endorsed by the PS of the Ministry (or Parent Ministry for statutory boards) in person. In this regard, MOF also issued two advisories: (i) to remind agencies to document their COVID-19 related EPs in a timely manner; and (ii) to guide agencies in managing existing contracts and suppliers that were impacted by the suspension of public services due to the Government's Circuit Breaker measures.

96 For COVID-19 schemes, the Committee noted that MOF and the Commercial Affairs Department (CAD) jointly issued an advisory to grant administering agencies, identifying potential fraud areas and recommending measures to mitigate fraud risk. These include pre-disbursement checks, as well as ex-post analytics and post-disbursement audit checks to identify potential fraud, abuse or conflicts of interest.

97 MOF informed the Committee that it is taking a multi-pronged approach to improve the Government's resilience in managing emergency situations whilst balancing with the need for fiscal prudence and accountability. MOF is reviewing its procurement policies and practices to identify the refinements needed, taking in lessons learnt from COVID-19. It is also working with the internal audit community to conduct ex-post analytics and audit checks on key COVID-19 related buys. In addition, MOF will work with procurement category leads to strengthen supply chain resiliency of critical goods and services required to effectively support public service delivery.

Ministry of Manpower

98 MOM informed the Committee that it had activated EP to support the urgent needs for related goods and services. MOM had put in place measures to manage the procurement process for such spending, without compromising operational responsiveness. Some of the measures adopted were:

a. Internal SOPs for Emergency Procurement

99 MOM had established clear processes and guidelines with key details such as the appropriate approving authorities for EP. In addition to existing controls and SOPs, MOM's Finance and Procurement teams also prioritised and checked through requests to ensure adequate oversight over MOM's COVID-19 expenditure.

b. Review of Procurement and Expenditure and Sampling Checks

100 MOM had also put in place controls to monitor COVID-19 spending, such as maintaining tracking spreadsheets and budget utilisation reports to monitor expenditures and aid officers in reconciling purchases with actual expenditures. MOM also planned to conduct sampling checks on the end-to-end process for COVID-19 expenditure by Q1 2021 to further strengthen its monitoring efforts.

c. Abide by Procurement Principles

101 MOM adopted the procurement principles of fairness, transparency and value-for-money by shortlisting suppliers from various sources where possible, evaluating suppliers based on their merits and performing cost comparisons to ensure prudence and accountability in the use of public funds.

102 Besides the measures elaborated above, MOM also informed the Committee that it relied on PPs and vendors to implement various COVID-19 support measures for individuals and businesses. Governance and control requirements were laid down through guidelines for scheme implementation, requiring segregation of duties with proper authorisation for grant disbursements, and monitoring efforts through regular reviews and post-disbursement checks. MOM is cognisant of the need for timely disbursements to grant recipients while maintaining accountability over public funds. Hence, MOM has instituted post-disbursement checks to detect any discrepancies. Key functions were conducted on-site to ensure proper data safeguards and supervision.

103 MOM had implemented the following measures to maintain adequate oversight and control:

a. Worked closely with vendors/PPs to discuss and formulate guidelines, to help ensure that the disbursement functions are performed according to the policy intent of the schemes;

b. Appointed external auditors to conduct pre-disbursement and/or post-disbursement checks;

c. Conducted regular check-ins with vendors and PPs for major schemes, to discuss cases, review work progress and identify areas for improvements; and

d. Implemented additional checks for major schemes through data analytics and anti-gaming framework to ensure the integrity of grant disbursements. Recipients who were found to have made erroneous declaration affecting their eligibility for grant pay-out would have their payment stopped and be asked to refund their grant monies.

Ministry of Trade and Industry

104 On financial assistance schemes that were introduced in response to COVID-19, MTI informed the Committee that it worked closely with its statutory boards and MOF to address potential risks by designing measures to mitigate such risks before actual implementation. For instance, for enhanced financing schemes such as the Temporary Bridging Loan, ESG has put in place a stringent assessment process before the financial

institutions are appointed as participating financial institutions (PFIs). ESG also required the PFIs to submit the loan applications through ESG's loans system that is designed with business rules to ensure that the schemes' eligibility criteria are met. ESG regularly monitors the take-up of the enhanced financing schemes, and submits regular reports to MTI and the BIC.

105 During the implementation stage, MTI works closely with the implementing statutory boards to balance operational flexibility while maintaining proper governance. For instance, in the area of enhanced financing schemes, the Chief Executive of ESG has been delegated with the authority to approve the applications that deviate from certain parameters within a given set of guidelines to ensure quick response on the ground. ESG must update MTI with a list of deviation cases approved by its Chief Executive. When these COVID-19 measures and initiatives conclude, the implementing agencies will conduct a post-implementation review through the Annual Consolidated Returns or the Project Closure Form that is submitted to MTI senior management.

106 MTI also informed the Committee that it had activated EP during the COVID-19 situation, which enabled its statutory boards to respond quickly to a fluid situation, while at the same time preserving accountability. MTI's agencies would also abide by the risk management protocols stipulated by MOF.

D. Future Risks

107 The Committee was concerned about the heightened risks brought about by disruptions caused by the COVID-19 pandemic, in particular risks in the area of public resources and risks arising from an acceleration of Government digital transformation initiatives.

108 On resourcing risks, the Committee asked MOF how it would address such risks, and whether there was a mechanism in place to re-evaluate the need and timeline for large-scale projects as some of the original projections may have changed significantly due to the COVID-19 pandemic.

109 On risks arising from the acceleration of digital transformation, the Committee asked SNDGG what are the new risks and areas of vulnerabilities that the agency had identified, the key scenarios considered when identifying these risks, and what measures it had taken to address or mitigate these risks.

110 The Committee also asked MCI, MOE, MOM and MTI on the key future risks from the management controls and financial spending perspective, and whether scenario planning was performed as part of their identification of future risks.

Resourcing Risks

Ministry of Finance

111 MOF informed the Committee that the need to address uncertainties and risks arising from COVID-19 was set in the context of sharper resource constraints. The Government had expended significant resources in its COVID-19 response and will face major constraints in its fiscal and manpower positions given weaker economic growth prospects, structural population ageing and international tax pressures. Amidst the tight fiscal and manpower positions, there will be smaller buffers available for any unforeseen needs.

112 MOF will work closely with agencies to reallocate resources more aggressively to create space for new priorities, and strengthen the strategy-resourcing loop in planning for major policy moves with significant resourcing needs. For example, MOF had been identifying areas of under-utilisation, and reviewing expenditures for which assumptions may have fundamentally changed, especially for large-scale projects.

113 On the re-evaluation of large-scale projects, MOF informed the Committee that the Government will continue to monitor the impact of COVID-19 on its long-term development plans and make suitable adjustments. There are inter-agency platforms that regularly review the longer-term planning assumptions. The Committee noted that for higher value projects, the Development Projects Advisory Panel would help to review specifications and design of large public sector projects to ensure that the planning assumptions are reasonable and public funds are used prudently.

114 The Committee also noted that the Strategy Group in the Prime Minister's Office drives WOG strategic planning by identifying key priorities and emerging issues over the medium to long-term. MOF is heavily involved to (i) ensure that fiscal considerations are adequately internalised in the scenarios, and (ii) factor any relevant scenarios in its medium-term fiscal planning.

Risks from Acceleration of Digital Transformation

Smart Nation and Digital Government Group

115 SNDGG informed the Committee that in line with the wider WOG ERM effort, it was in the process of establishing a WOG ICT&SS ERM system comprising (i) a central WOG ICT&SS ERM office, (ii) risk owners for each identified prioritised risk, and (iii) integration of the WOG risk framework into agency-level ERM processes by all Government agencies.

116 For risk identification, SNDGG performed both external and internal risk scanning. These include research from ERM experts, risks published by technology companies and data points gathered from agencies. SNDGG had identified ten risks, which include human capital risk, technology development risk, cybersecurity risk and third-party risk.

117 SNDGG also informed the Committee that COVID-19 had been a stress test of digital capabilities and brought to the fore risks such as tech and data exploitation risk, technology development risk and digital access risk. At the same time, defensive risks such as cybersecurity risk and data security risk will need to be addressed as digitalisation is accelerated and reliance on digital systems is increased.

118 SNDGG informed the Committee that most of the identified risk domains have been or are being addressed by its ongoing efforts. These include strengthening central and agency governance of ICT&SS risks, strengthening agencies' management of data security and cybersecurity risks, and managing human capital risks.

Key Future Risks

Ministry of Communications and Information

119 MCI informed the Committee that its scenario planning focuses on long-term horizon scanning for external risks and threats. A key area of work in futures and scenario planning involve long-term horizon scanning in MCI-related domains for external risks and threats. This risk identification continuously examines the external environment to enable MCI to develop a comprehensive sensing of nascent trends and contextualise their potential impact on the MCI Family's work.

120 The shorter-term corporate planning process at MCI is built around an internal workplan cycle. This is an iterative process reported annually to senior management. Under this workstream, MCI Divisions identify core/programme-level risks for their

work and map out their potential consequences. They are subsequently required to generate plans to manage and mitigate these risks.

121 For effective resource allocation and proper accountability of funds, MCI has a structured monitoring and evaluation process to assess the performance of government funded projects or programmes. This includes a bi-annual "Project Monitoring Framework", where potentially problematic projects are included in the Project Monitoring Watchlist for closer monitoring.

Ministry of Education

122 On scenario planning, MOE informed the Committee that it keeps abreast of emerging trends and innovative practices overseas to distil learning points for Singapore. MOE is also plugged into the broader WOG futures community that does scenario planning at the WOG level.

Ministry of Manpower

123 MOM informed the Committee that it proactively identifies and addresses emerging risk areas through its risk management framework. Responding to the Committee, MOM shared that it is already preparing to re-think existing strategies to strengthen its support for vulnerable segments such as low-wage workers, and to cope with the higher risk of structural unemployment. At the organisation level, MOM tracks Key Risk Indicators to address strategic and operational risks in its key pillars of work. This is further supported by MOM's three Lines of Defence, namely "Department-level Compliance and Alignment", "Quality Control and Consistency", and "Independent Assurance". This framework would operationalise risk management and ensures financial governance through accountability and governance at all levels.

Ministry of Trade and Industry

124 MTI informed the Committee that in the short-term, the main risks relate to economic recovery from the COVID-19 pandemic. MTI uses a variety of frameworks to guide its longer term strategic planning, including scenarios. MTI looks at economic driving forces and develops scenarios which challenge the operating models and policy assumptions. MTI also simulates baseline, upside, and downside growth trajectories for the global and domestic economies over the next one to two years, based on multiple factors.

125 MTI also informed the Committee that risk management is performed at the senior management levels. Within the MTI family, there are regular discussions between the senior management of MTI-HQ and statutory boards on key strategies and initiatives, and the tracking of KPIs. For instance, each statutory board submits a Progress Update every quarter to MTI-HQ, tracking the progress of their programmes. Regular updates on key projects are also submitted via staff channels for all parties' information.

Appendix I

MINUTES OF PROCEEDINGS

1st Meeting

Tuesday, 27 October 2020

1.30 p.m.

PRESENT:

Ms Foo Mee Har (*in the Chair*)
Miss Cheryl Chan Wei Ling
Mr Chua Kheng Wee Louis
Mr Derrick Goh
Mr Kwek Hian Chuan Henry
Ms Poh Li San
Mr Saktiandi Supaat
Dr Tan Wu Meng

---

1. The Committee considered the Report of the Auditor-General for the Financial Year 2019/20 (Paper Cmd. 1 of 2020).

2. The Committee deliberated.

3. The Committee examined the findings contained in the Auditor-General's report and agreed to write to the Ministry of Communications and Information, Ministry of Education, Ministry of Finance, Ministry of Manpower, Ministry of Trade and Industry and the Prime Minister's Office to submit memoranda on matters raised.

Adjourned to 4 December 2020.

2nd Meeting

Friday, 4 December 2020

10.30 a.m.

PRESENT:

Ms Foo Mee Har (*in the Chair*)
Miss Cheryl Chan Wei Ling
Mr Chua Kheng Wee Louis
Mr Derrick Goh
Mr Kwek Hian Chuan Henry
Ms Poh Li San
Mr Saktiandi Supaat

ABSENT:

Dr Tan Wu Meng

---

1. The Committee considered the memoranda received from the Ministry of Communications and Information, Ministry of Education, Ministry of Finance, Ministry of Manpower, Ministry of Trade and Industry and the Prime Minister's Office.

2. The Committee deliberated.

3. The Committee agreed to write to the Ministry of Communications and Information, Ministry of Education, Ministry of Finance, Ministry of Manpower, Ministry of Trade and Industry and the Prime Minister's Office to submit further memorandum on matters raised. The Committee also agreed that the Permanent Secretary of the Ministry of Finance and the Permanent Secretary of the Ministry of Manpower be invited to give oral evidence at the next meeting.

Adjourned to 17 December 2020.

3rd Meeting

Thursday, 17 December 2020

10.30 a.m.

PRESENT:

Ms Foo Mee Har (*in the Chair*)
Miss Cheryl Chan Wei Ling
Mr Chua Kheng Wee Louis
Mr Derrick Goh
Mr Kwek Hian Chuan Henry
Ms Poh Li San
Mr Saktiandi Supaat

ABSENT:

Dr Tan Wu Meng

---

1. The following officials were examined on matters contained in the memoranda:

Ministry of Finance
(i) Mr Yee Ping Yi, Deputy Secretary (Planning)
(ii) Mr Han Neng Hsiu, Deputy Secretary (Development)
(iii) Mr Chia Ser Huei, Chief of Government Procurement and Director
(iv) Mr Koh Kok Liang John, Programme Director (Grants Governance Office)
(v) Mr Chin Yi Zhuan, Deputy Director (Fiscal Policy) and Deputy Director (Strategic Communications and Engagement)

Ministry of Manpower
(i) Mr Aubeck Kam, Permanent Secretary
(ii) Mr Foo Kok Jwee, Deputy Chief Executive (Workforce Singapore)
(iii) Mr Jason Tay Lian Sen, Director (Enterprise Programmes Division, Workforce Singapore)
(iv) Ms Yak Keng Hoon, Deputy Director (Finance)
(v) Ms Ang Tiong Ling, Head (Internal Audit)

2. The Committee deliberated and considered the Chairman's draft report.

Adjourned to 26 January 2021.

4th Meeting

Tuesday, 26 January 2021

10.30 a.m.

PRESENT:

Ms Foo Mee Har (*in the Chair*)
Mr Chua Kheng Wee Louis
Mr Derrick Goh
Mr Kwek Hian Chuan Henry
Ms Poh Li San
Mr Saktiandi Supaat

ABSENT:

Miss Cheryl Chan Wei Ling

---

1. The Committee considered the further replies received from the the Ministry of Communications and Information, Ministry of Education, Ministry of Finance, Ministry of Manpower, Ministry of Trade and Industry and the Prime Minister's Office.

2. The Committee deliberated.

Report

3. The Chairman's report brought up and read the first time.

4. Resolved, "That the Chairman's report be read a second time paragraph by paragraph.".

5. Paragraphs 1 to 125 inclusive read and agreed to.

6. Resolved, "That this report be the report of the Committee to Parliament.".

7. Agreed that the Chairman do present the Report to Parliament when copies are available for distribution to Members of Parliament.

Adjourned sine die.